1994-09

Leveraging Naval Riverine forces to achieve information superiority in stability operations

Gray, Stephen C.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

LEVERAGING NAVAL RIVERINE FORCES TO ACHIEVE INFORMATION SUPERIORITY IN STABILITY OPERATIONS

by

Stephen C. Gray

December 2010

Thesis Advisor:	R. Mitchell Brown III
Second Reader:	Karl D. Pfeiffer

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Leveraging Naval Riverine Forces to Achieve Information Superiority in Stability Operations			**5. FUNDING NUMBERS**
6. AUTHOR(S) Stephen C. Gray			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ___N.A.___.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The conflicts of Iraq and Afghanistan have provided an undeniable storyline: U.S. forces can conduct a conventional mission better than any in the world, but that mission, accomplished in short order, leaves behind a situation for which conventional forces and equipment are ill-prepared. This situation requires a new mission: Stability Operations. The blue-water is not where these 21st century conflicts will likely take place, and forces such as the U.S. Navy Riverines are among the many forces that provide a capability to integrate and communicate with local populations that cannot be matched by blue-water forces. While the riverine force's mission set is one that could become heavily utilized in stability operations, the ability to conduct those missions is currently hindered by a lack of implementation of information technology. The current disadvantages that greatly increase operational risk include a reduced capability to engage the population, reduced situational awareness, and limited communication reach-back capability. A riverine force properly equipped with and trained with biometric, unmanned, and information sharing systems would provide the NECC, and U.S. Navy as a whole, a more comprehensive ability to conduct stability operations in brown-water areas, something no other conventional Navy unit can currently accomplish.

14. SUBJECT TERMS Riverine, Security, Stability, Transition, and Reconstruction Operations, Information Superiority, Naval Expeditionary Combat Command, Biometrics, Unmanned Aircraft Systems, Unmanned Aerial Vehicle, Unmanned Surface Vehicles, Information Sharing, Information Technology, Irregular Warfare, Asymmetric Warfare			**15. NUMBER OF PAGES** 124
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 8-98) Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

LEVERAGING NAVAL RIVERINE FORCES TO ACHIEVE INFORMATION SUPERIORITY IN STABILITY OPERATIONS

Stephen C. Gray
Lieutenant, United States Navy
B.S., Virginia Tech, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
December 2010

Author: Stephen C. Gray

Approved by: R. Mitchell Brown III
Thesis Advisor

Karl D. Pfeiffer, PhD
Second Reader

Dan C. Boger, PhD
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The conflicts of Iraq and Afghanistan have provided an undeniable storyline: U.S. forces can conduct a conventional mission better than any in the world, but that mission, accomplished in short order, leaves behind a situation for which conventional forces and equipment are ill-prepared. This situation requires a new mission: Stability Operations. The blue-water is not where these 21st century conflicts will likely take place, and forces such as the U.S. Navy Riverines are among the many forces that provide a capability to integrate and communicate with local populations that cannot be matched by blue-water forces. While the riverine force's mission set is one that could become heavily utilized in stability operations, the ability to conduct those missions is currently hindered by a lack of implementation of information technology. The current disadvantages that greatly increase operational risk include a reduced capability to engage the population, reduced situational awareness, and limited communication reach-back capability. A riverine force properly equipped with and trained with biometric, unmanned, and information sharing systems would provide the NECC, and U.S. Navy as a whole, a more comprehensive ability to conduct stability operations in brown-water areas, something no other conventional Navy unit can currently accomplish.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAR	After Action Report
ASW	Anti-Submarine Warfare
BAT	Biometric Automated Toolset
BIMA	Biometrics Identity Management Agency
BFT	Blue Force Tracker
BTF	Biometrics Task Force
C4I	Command, Control, Communications, Computers, and Intelligence
CALL	Center for Army Lessons Learned
CBR	Chemical, Biological, and Radiological
CENTRIXS	Combined Enterprise Regional Information Exchange System
CIMILink	Civil-Military Link
COIN	Counterinsurgency
COP	Common Operational Picture
DoD	Department of Defense
DON	Department of the Navy
DSU	Dam Security Unit
ECP	Entry Control Point
EFP	Explosively Formed Penetrator
EOD	Explosive Ordnance Disposal
FOB	Forward Operating Base
FY	Fiscal Year
GAO	Government Accountability Office
GCE	Ground Combat Element
GPS	Global Positioning System
HA/DR	Humanitarian Assistance and Disaster Relief
HIIDE	Hand-Held Interagency Identification Detection Equipment

HLZ	Helicopter Landing Zone
HQ	Headquarters
IED	Improvised Explosive Device
IGO	International Government Organization
IOC	Initial Operational Capability
ISIC	Immediate Superior in Command
ISR	Intelligence, Surveillance, and Reconnaissance
JCA	Joint Capability Area
JCS	Joint Chiefs of Staff
JOC	Joint Operating Concept
JP	Joint Publication
LOS	Line of Sight
MCM	Mine Countermeasures
MCO	Major Combat Operations
MDA	Maritime Domain Awareness
MEDEVAC	Medical Evacuation
METOC	Meteorological and Oceanographic
MSO	Maritime Security Operations
MWD	Military Working Dog
NAVAIR	Naval Air Systems Command
NCIS	Navy Criminal Investigative Service
NECC	Naval Expeditionary Combat Command
NGO	Non-Governmental Organization
NMET	Navy Mission Essential Task
NMETL	Navy Mission Essential Task List
NTS 2000	Non-Combatant Evacuation Operation Tracking System 2000
NTTP	Navy Tactics, Techniques, and Procedures
OIC	Officer in Charge
OIF	Operation Iraqi Freedom

OPLAN	Operational Plan
OPNAV	Office of the Chief of Naval Operations
PMO	Program Management Office
POSREP	Position Report
POST	Peace Operations Support Tool
PRT	Provincial Reconstruction Team
QDR	Quadrennial Defense Review
RIVGRU	Riverine Group
RIVRON	Riverine Squadron
RFI	Request For Information
RMIO	Riverine Maritime Interdiction Operations
RPB	Riverine Patrol Boat
SEAD	Suppression of Enemy Air Defenses
SFA	Security Force Assistance
SHARE	Structured Humanitarian Assistance Reporting
SIGACT	Significant Action
SIGINT	Signals Intelligence
SIPRNET	Secret Internet Protocol Router Network
SITREP	Situation Report
SOA	Speed of Advance
SSE	Sensitive Site Exploitation
SSTR	Stabilization, Security, Transition, and Reconstruction
SSTRO	Stabilization, Security, Transition, and Reconstruction Operations
STUAS	Small Tactical Unmanned Aircraft System
SWO	Surface Warfare Officer
TAO	Tactical Action Officer
TOA	Table of Allowances
TSE	Tactical Site Exploitation
TTP	Tactics, Techniques, and Procedures

UAS	Unmanned Aircraft System
UGV	Unmanned Ground Vehicle
UMS	Unmanned Maritime System
UNICEF	United Nations Children's Fund
USA	United States Army
USG	United States Government
USMC	United States Marine Corps
USN	United States Navy
USV	Unmanned Surface Vehicle
UUV	Unmanned Undersea Vehicle
WBGP	Waterborne Guard Post
WMD	Weapons of Mass Destruction

ACKNOWLEDGMENTS

First and foremost, I owe the greatest thanks to my wife, Darcy Gray. Without her steadfast and unwavering support, this would not have been possible. She encouraged me, motivated me, and never let me quit. I owe this thesis to her.

I would also like to thank Keith Paquin, a fellow riverine who epitomizes a great Naval Officer. We went to Iraq and Monterey together, and both times we found many occasions to depend on each other. I am thankful for his friendship, his advice, and the many hours he spent reviewing this thesis.

I owe a great thanks to my thesis advisor, Professor Mitch Brown, and my second reader, Lt. Col. Karl Pfeiffer. Without your great help, I might have failed in this endeavor. Thank you for taking on the role of making sure I succeeded in the face of adversity.

Lastly, I would like to thank my NPS classmates from the IST curriculum. Justin Hayward, Lillian Abuan, Ryan King, Jeff Bennington, Dalton Clarke, James Fisher, Devine Johnson, you each made all the long hours and hard work worth it. We succeeded at NPS as a team and I will miss you as we each go our separate ways.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

As the first decade of the 21st century fades, the revelation that the conflicts that will shape this new century will be very different from the last has become apparent. The U.S. military faces two fundamental challenges as it confronts the challenges of contemporary conflict.

First, the nature of warfare has changed. No longer will battlefields exist where masses of forces face each other head-to-head. No longer constrained by geography, the new battlefield is multidimensional, made up of regions of conflict to include land, sea, air, space, and cyberspace. The foes of the United States are not massed on a field or in a city. They are agile, hidden from plain view, leverage global black-market, criminal, and terrorist networks, strike at new centers of gravity such as public opinion, and use U.S. technology dependency to their advantage. Opposition forces know that to win, they must draw the United States into prolonged conflict, make the United States attempt the challenge of turning failed states into functioning democracies, and use the imperfections and horrific tolls of warfare to provide a relentless fuel for their information war in efforts to destabilize support for U.S. operations from both foreign and domestic audiences.

The second challenge the U.S. military faces is internal. The United States enjoys superior capability in forces, ships, aircraft, armor, etc., but they were all designed to meet the challenges of the last century. The conflicts of Iraq and Afghanistan provide an undeniable storyline: U.S. forces can conduct conventional missions better than any in the world. But those missions must be accomplished in short order, because sustained combat operations leave conventional forces ill-equipped and ill-prepared. These situations led into a new mission area of Stability Operations. Stability operations are a fundamental mission that the military must be prepared to conduct in the 21st century. As discussed by Benbow, Ensminger, Swartz, Savitz, and Stimpson (2006), to face

this challenge, many things must change: doctrine, tactics, techniques, and procedures (TTP) must be revised; personnel must be available, trained, and educated; the logistics of supplies, maintenance, and infrastructure must be updated; and new systems, equipment, and vehicles need to be acquired.

In order to meet these two challenges head-on, a fundamental question must be answered. How can the Department of Defense (DoD) adapt to the new nature of contemporary conflict? The approach taken in the latter parts of Operation Iraqi Freedom (OIF), and since General McCrystal's arrival in Afghanistan in the spring of 2009, has laid the foundation of how asymmetric warfare[1] will be conducted in the 21st century. More important than the use of conventional weapons and tactics, is how leveraging of information and communication with the local population has taken the forefront. This new emphasis on communication and relationship building with local leaders requires U.S. forces to operate in such a way that they are embedded with the population, an environment that is rich in information. To appropriately gather this information so it can be quickly utilized and then consolidated, analyzed, and shared with others, requires technology and techniques that are just recently starting to gain traction in the military.

The vast requirements that must be fulfilled by the DoD in order to collect and leverage this information, thereby allowing for a more effective effort toward challenges of contemporary conflict, are beyond the scope of this thesis. However, this thesis will argue that the close examination of how one particular type of unit should be supplemented and adapted, can provide a construct for adapting other units in a similar manner. The specific unit intended for exploration, and how they could be adapted to be a more effective force in contemporary conflict, is the U.S. Navy Riverine Forces.

1 Asymmetric warfare–Warfare that displays a "disproportion of strength between the opponents at the outset, and from the difference in essence between their assets and liabilities" (Galula, 1964).

The Navy's Riverine forces have a rich history of serving meritoriously in various conflicts, while being subjected to budgetary chopping blocks when these conflicts cease. The fundamental reasoning behind such actions is that support for small river forces has difficulty competing with the rich, blue-water culture and tradition that runs through the Navy's veins, and defense budgets that are artificially inflated during conflict. The truth of the matter, though, is that the blue-water is not where conflict in the 21st century will likely take place, and that forces such as riverines are among the many Navy Expeditionary Combat Command (NECC) forces that provide a capability to integrate and communicate with local populations, unmatched by blue-water forces. This pronounced capability enables joint force commanders to utilize riverine forces to obtain and share information vital to attaining battlespace information superiority, a distinct and unique advantage.

While the riverine force's mission set is one that should become heavily utilized in stability operations, the ability to conduct those missions is currently hindered. Chapter II will describe and discuss stability operations and how riverine forces have a broad set of capabilities useful in performing those operations. Additionally, the inherent limitations to what riverine forces can accomplish with the systems, equipment, and training they currently employ and the operational risk that is associated with this shortfall will be discussed. The remaining chapters will argue that in order to reduce operational risk, the riverine forces should be supplemented with biometric, unmanned, and information sharing systems. This enhanced capability will provide the joint force commander a significantly more valuable asset in which to leverage in stability operations.

A. RESEARCH QUESTION

The U.S. Navy must find ways to use their most agile and adaptable forces to accomplish missions that blue-water forces cannot complete. This

research will examine how the Naval Riverine Forces can provide a more effective information superiority capability to the joint force commander in stability operations.

B. RESEARCH OBJECTIVE

The objective of this research is to analyze the current capabilities and limitations of the U.S. Navy Riverine Forces, and explain how they could be supplemented with new and emerging information technologies to enable them to become a force-multiplier in achieving information superiority in the joint battlespace.

C. SIGNIFICANCE OF RESEARCH

A properly equipped and trained riverine force would provide the NECC, and U.S. Navy as a whole, an improved ability to conduct stability operations in brown-water areas, something no other conventional Navy unit can accomplish. This capability is needed in order to make a valid and convincing argument for the continued retention of Naval Riverine capability after Operation Iraqi Freedom is concluded. Ultimately, the value of the improved capability that is brought is much higher than the relatively small investment in dollars and people. If implemented, the riverine forces will be cost effective, highly sought, and ably equipped to respond to joint force requirements in future stability operations.

D. THESIS ORGANIZATION

This thesis will examine the expanded mission capability gained by the U.S. Riverine Forces when supplemented with emerging technology. Chapter II will discuss the capabilities and limitations of the riverine forces as they are currently trained and equipped. Chapter III will describe the capabilities that could be gained through the utilization of biometric systems. Chapter IV will provide feedback on how the expanded use of unmanned systems by the riverine forces could be advantageous. Chapter V will discuss how information sharing

systems will allow supporting and supported units to take advantage of the collection capabilities of the riverine force. Finally, Chapter VI will present a future enhanced riverine force that has executed an influx of emerging information technologies that will provide a vision for NECC and any other type commander who desires to prepare their small units for the stability operations that the 21st century will bring.

E. METHODOLOGY AND SOURCES

This thesis will consist of a review of U.S. National Defense Strategy, maritime strategy, and U.S. Department of Defense and Joint Force doctrine, directives, instructions, and publications. Additionally, various resources utilized by the creators and subsequent commanders of the newly re-established riverine force investigating riverine force make-up, equipage, training, and mission set will be reviewed. Lastly, various Naval Postgraduate School theses that discuss implementation of emerging technology in the maritime domain will be examined.

THIS PAGE INTENTIONALLY LEFT BLANK

II. RIVERINE FORCE CAPABILITIES AND LIMITATIONS

A. STABILITY OPERATIONS

Stability operations,[2] also sometimes referred to as Stabilization, Security, Transition, and Reconstruction (SSTR) Operations, describe the range of operations that occur beyond the scope of peace operations, but short of the scope required for combat operations. The U.S. JCS (2006) says that stability operations:

> Focuses on the full range of military support that the future Joint Force might provide in foreign countries across the continuum from peace to crisis and conflict in order to assist a state or region that is under severe stress or has collapsed due to either a natural or man-made disaster. A SSTR operation is not solely a military effort, but rather one that requires a carefully coordinated deployment of military and civilian, public and private, U.S. and international assets.

In order to advance U.S. government interests in a region and secure a lasting peace, there are various options that exist for military support to stability operations. The following are a collection of possible activities that the U.S. JCS (2006) believes the U.S. Military could complete in support of stability operations:

- Assist an existing or new host nation government in providing security, essential public services, economic development, and governance following the significant degradation or collapse of the government's capabilities due to internal failure or as a consequence of the destruction and dislocation of a war;[3]

[2] Stability operations–An overarching term encompassing various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (U.S. JCS, 2001)

[3] In the case of the beleaguered fragile government, noted above, the armed opposition may take the form of an insurgency. In such cases, the SSTR operation is called a counterinsurgency (COIN) operation.

- Provide support to stabilize and administer occupied territory and care for refugees in major combat operations fought for limited objectives that fall short of forcibly changing the adversary regime;
- Support a fragile national government that is faltering due to serious internal challenges, which include civil unrest, insurgency, terrorism and factional conflict;
- Assist a stable government that has been struck by a devastating natural disaster;
- Provide limited security cooperation assistance to a state that is facing modest internal challenges; and
- Provide military assistance and training to partner nations that increase their capability and capacity to conduct SSTR operations at home or abroad.

B. RIVERINE FORCE INTRODUCTION AND CAPABILITIES

1. Introduction

Riverine forces began their recent resurgence back into operational duty in 2006. Deactivated since the Vietnam conflict, new riverine forces were created to fill a capability gap that was recognized during OIF. Riverine Group (RIVGRU) One and Riverine Squadron (RIVRON) One were both established in 2006, with RIVRONs 2 and 3 following soon after in 2007. NECC (2010), which serves as RIVGRU One's Immediate Superior in Command (ISIC), describes the riverine force as follows:

- Three Riverine Squadrons, under one Riverine Group Commander, serve as a ready force for the Joint Forces Maritime Component Commander or Joint Forces Land Component Commander.
- Each Riverine Squadron consists of specially designed craft, vehicles and unmanned systems configured to operate in a hostile riverine environment. The craft have multiple crews for near continuous operations and lift capacity for a small tactical unit. The headquarters element provides organic command, control, communications, computers and intelligence, force protection and logistics.
- The Riverine Force provides the ability to conduct combat operations against small tactical, waterborne and unconventional

warfare units in a riparian environment and security force assistance and training to friendly nations.

As will be discussed, riverine forces were designed to operate in all operations short of engaging a large enemy tactical force. This design coupled with the NECC (2010) vision of riverine operations argues that they represent the exact type of force that would be needed to support stability operations.

> The nature of riverine operations requires forces tailored and packaged for the mission and environment assigned to the operational commander including maritime security operations (MSO) and security force assistance (SFA). MSOs deny violent extremist and criminal networks the use of the maritime environment as a venue for attack or to transport personnel, weapons or other material, and set the conditions for security and stability of regional nations. SFA entails protecting critical infrastructure; securing the area for military operations or commerce; preventing the flow of contraband; enabling power projection operations; joint, bilateral or multilateral exercises; conducting personnel exchanges; and participating in humanitarian assistance.

2. Objectives

According to DoD Instruction 3000.5, Stability Operations (2009), the DoD must be able to:

- Establish civil security and civil control.
- Restore or provide essential services.
- Repair critical infrastructure.
- Provide humanitarian assistance.

While these objectives are quite broad, riverine forces can have a major impact in two of these areas: civil security/control and humanitarian assistance. The other two, restore/provide services and repair infrastructure, are more selective in the forces that would be required, but riverine forces are always able to assist in waterborne security and logistical support for virtually any mission in which they are not the main effort. There are various missions included in the subset of the objectives outlined above. As Oliver (2008) shows, these include

show of force, counterinsurgency, and counterterrorism as part of civil security/control and peace operations and non-combatant evacuation as part of humanitarian assistance. Whatever the mission, there are tasks from the Navy Mission Essential Task List (NMETL) that comprise the various aspects of that mission. All Navy Mission Essential Tasks (NMETs) that apply to Riverine Forces are shown in Table 1.

NAVY TACTICAL TASK	NAVY MISSION-ESSENTIAL TASK	TYPE OF OPERATION			
		Maritime Security	Patrolling and Interdiction	Theater Security Cooperation	Assault Support
1.1.2.3	Move Units	X	X	X	X
1.1.2.3.4	Conduct Convoy Operations	X	X	X	X
1.1.2.3.7	Conduct Small Boat Operations	X	X	X	X
1.1.2.4	Conduct Tactical Insertion and Extraction		X		X
1.2	Navigate and Close Forces	X	X	X	X
1.4.6	Conduct Maritime Interception	X	X		
1.4.7	Enforce Exclusion Zones	X		X	
1.5.5.5.4.1	Secure an Area	X	X	X	X
1.5.5.6.1	Conduct Patrols	X	X	X	X
2.1.3	Conduct Collection Planning and Directing		X		
2.2	Perform Collection Operations and Management	X	X	X	X
2.4.4.4	Evaluate the Threat	X	X	X	X
2.5	Disseminate and Integrate Intelligence	X	X	X	X
3.1.1	Request Attack	X	X	X	X
3.1.5	Conduct Tactical Combat Assessment		X		X
3.2	Attack Targets	X	X		X
3.2.8.2	Illuminate/Designate Targets	X	X		X
3.2.9	Conduct Nonlethal Engagement	X	X		X
4.12.1	Perform Triage	X	X	X	X
4.12.11	Provide Medical Staff Support	X	X	X	X
4.12.2	Provide Ambulatory Health Care	X	X	X	X
4.12.5	Coordinate Patient Movement	X	X	X	X
4.12.9	Train Medical and Nonmedical Personnel	X	X	X	X
4.3	Repair/Maintain Equipment	X	X	X	X
5.1.1.1	Transmit and Receive Information	X	X	X	X
5.2.1.2	Review and Evaluate Mission Guidance	X	X	X	X
5.2.1.3	Review Rules of Engagement	X	X	X	X
5.3	Determine and Plan Actions and Operations	X	X	X	X
5.4.4	Establish Liaisons	X	X	X	X
6.1.1.1	Protect Individuals and Systems	X	X	X	X
6.3.2.1	Manage Enemy Prisoners of War	X	X		X
6.3.3	Combat Terrorism	X	X	X	

Table 1. U.S. Navy Riverine Mission-Essential Tasks (From U.S. Department of the Navy (DON), 2008)

These essential tasks are still broadly defined and are subject to unit TTPs on how to effectively complete them, but they do provide a baseline from which to identify where current capabilities and limitations are affecting the ability to accomplish any given mission. It should be noted that Table 1 does not include stability operations, but each of the four operations mentioned in the table would be expected to be accomplished during the conduct of stability operations.

3. Capabilities

There are some key capabilities inherent with riverine forces that make them ideal for stability operations. First and foremost is the operational area in which they are able to operate. Riverine forces are able to fill a critical gap between where traditional land and maritime forces can effectively operate. These areas include rivers, deltas, harbors, canals, and many others. This gap is especially crucial, because these riverine areas provide essential needs to the local population. As Benbow et al. (2006) describes, these areas "sustain life with food and water, support agriculture, and provide a means of transportation and energy production." These areas also serve an even more crucial role in transportation, when traditional land-based transportation is limited or destroyed by natural disasters or conflict. Because these areas are so important and are home to significant segments of the population, they can also serve as a key operational area during stability operations.

In addition to access to areas that prove difficult for land units to reach, riverine areas allow for a speed to be achieved that is much greater than what can be achieved on land. Currently, riverine assets regularly transit at 30 to 35 knots. The reason this speed is possible is because the threat is limited by the terrain. Where the transit area is wide, the threat is limited by the effective range of the weapons in use; where the transit area is narrow, the speed limits the time in which the riverine asset is able to be identified and targeted. Additionally, as technology has made the creation and use of improvised explosive devices (IEDs) more common along the roadways, the speed with which units can

operate on land has become even more constrained. Speed is not only an asset in avoiding threats, but also in the ability to conduct operations in which time is of the essence, particularly for humanitarian assistance and disaster relief (HA/DR). The ability to conduct medical evacuation (MEDEVAC) and transportation of supplies, such as food and water at increased speed of advance (SOA), drastically increases the number of people who are able to be assisted over that of ground units.

The next capability that riverine forces have that makes them unique in stability operations is their ability to operate both on water and on land. The significance of this is hard to overstate. Other platforms, rotary wing aircraft for example, are also highly mobile, but have very limited ability to operate in a manner that focuses on putting foot-mobile forces on the ground, as a regular occurrence. On the opposite end of the spectrum, land-based units are quite easily able to put units on the ground for missions of diverse length, but their mobility is limited. Riverine forces provide a capability that offers a mix of mobility and access. The current craft in use, the Riverine Patrol Boat (RPB), shown in Figure 1, is able to push directly onto the shoreline to unload its compliment of the embarked RMIO team.

Figure 1. Riverine patrol boat (From Stone, 2009)

The RMIO team is designed to be a specialized and highly trained component of the RIVRON that is able to conduct operations ashore to include sweep and clear, cordon and search, MEDEVAC, detainee operations, and many more. One of the most effective uses of the RMIO team is as an engagement force. They have the ability to operate among the population ashore, providing the crucial communication capability that would not be able to take place from the riverine craft alone.

C. RIVERINE FORCE LIMITATIONS AND CONSTRAINTS

1. Key Limitations

While the U.S. Navy (USN) riverine forces do bring a unique capability to the joint force commander, they currently have limitations that prevent them from becoming as effective a unit as they could be. The first limitation is a reduced capability of the RMIO team to engage the population. One of the major problems that the RMIO team suffers from is that they have no way to identify the people they are talking to, either on other watercraft or ashore. This, at first glance, seems to be fairly insignificant, but when coupled with severe language barriers, there exists an inability to attribute any information gathered with any degree of certainty. This problem is further exacerbated when RMIO teams conduct repeat engagement in a given area so infrequently. This situation makes collaborating information gathered during two different patrols dependant solely on the memory of the patrol members. Beyond collaborating past and present engagement activities, there is a fundamental lack of integrity in the process of verifying the identity of the individual in question. The ubiquity of government issued identification varies widely and the forging of government identification is always of concern.

The second key limitation that the riverine forces suffer is increased risk of attack and reduced situational awareness, stemming from what is a limited ability to identify with certainty what lies beyond LOS. This weakness stems from the

lack of dedicated air support for the RIVRON. Without this level of support, both the riverine craft and RMIO team are vulnerable during operations. This vulnerability stems from the fact that rivers, by their very nature, are in defilade. Always having to operate in a position that leaves a unit open to attack from above, with limited ability to effect direct fire, is dangerous. To add to the danger of the terrain, a riverine unit only has two directions in which to travel most times, upstream and downstream. Being able to travel in only two directions has two fundamental flaws. First, the enemy only has two choices to affect their force placement decisions and second, riverines that travel upstream must follow along the same path to return to base. These disadvantages in terrain make it extremely important that riverine forces have some additional ability to see beyond LOS, making it possible to avoid enemies lying in wait along the river.

The last fundamental limitation suffered by the riverine forces is communication reachback capability. During operations, there are multiple instances in which there is information, such as documents, photos, and maps that need to be sent to, and/or from HQ and the operating riverine forces. The inability to send and/or receive this information severely limits the information with which the riverine forces are able to operate. On the force's side, mission plans and details have to be either memorized, or brought in a very vulnerable paper format. While planning documents can be arranged to be brought on mission, there is little capability to acquire amplifying or new data to assist in reacting to situations as they change. HQ suffers from the same lack of information coming from the operating unit. With communications limited to voice only, HQ operates on periodic position reports (POSREPs) and occasional situation reports (SITREPs). They have no ability to access any video, audio, or documents obtained by the boat or RMIO team. This problem prevents the intelligence personnel with the RIVRON from being able to provide real time analysis, or updates based off real-time events. Overall, the communication between operating forces and the HQ is extremely limited, meaning that tactical control of the operating force is very difficult, if not impossible to manage.

2. Timing

In addition to the considerations of what mission is being conducted, riverine forces will be utilized only during specific phases of the operation. U.S. DON Tactics, Techniques, and Procedures (NTTP) 3.06-1 (2008) states:

> Riverine forces are not manned, trained, and equipped for forcible entry operations or large-scale offensive and defensive operations. Significantly, the introduction of Navy riverine forces into a theater of operations requires an established forward operating base (FOB) or a forward logistic site, which can be land- or sea-based, from which to operate.

This requirement coincides with the general status that exists in phase IV and phase V operations, with the possibility of existing in late phase III. While the U.S. Joint Chiefs of Staff (JCS) Joint Publication (JP) 3-0 (2008) does not specifically break out different phasing models for combat and non-combat operational plans (OPLANs), the model can be applied and interpreted for both (Figure 2).

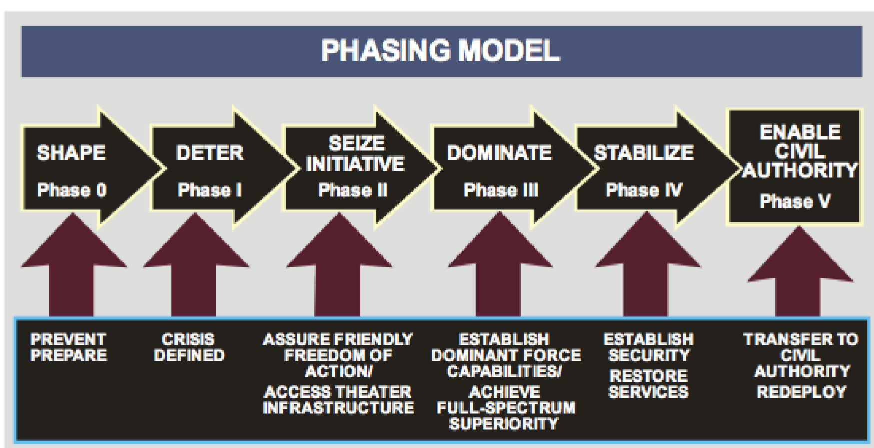

Figure 2. Phasing model (From U.S. JCS, 2008)

These prerequisites put into place for planners' consideration are mutually supporting to the same phases that would be implemented by the majority of actors conducting stability operations in theater. As Oliver (2008) describes, it is understood that while Major Combat Operations (MCO) are underway, in phase

III, most actions inherent in stability operations will be secondary in nature. As Figure 3 shows, and as discussed by Oliver (2008), as phase III ends, stability operations will increase in size, duration, and importance. It should be noted that the timing for the ending of phase III can be abrupt, so preparations for the stability operations that will occur in phase IV must be implemented and ramped up during phase III. Case in point is the abrupt end to MCO during OIF, which lasted only 43 days compared to the length of the overall campaign, which ended in its seventh year in 2010.

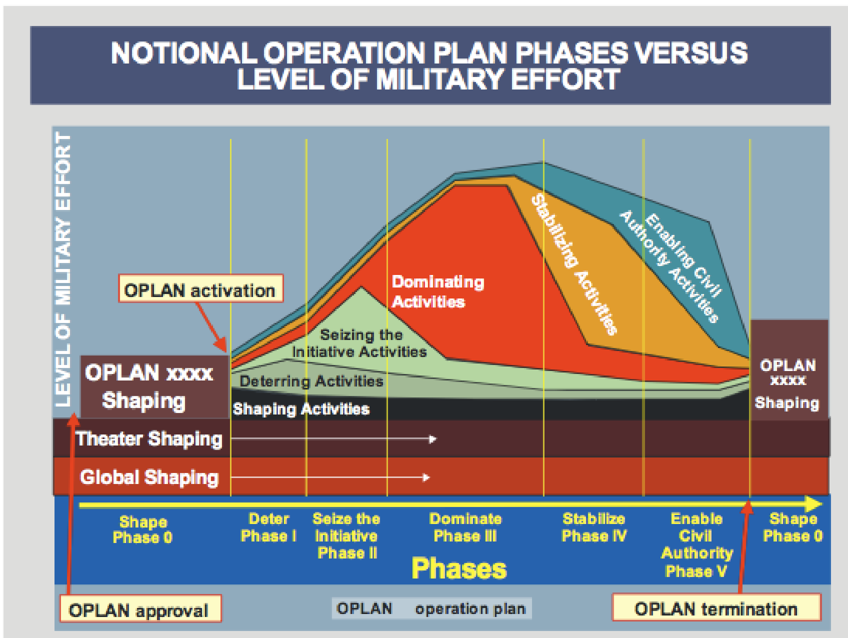

Figure 3. Notional operation plan phases versus level of military effort (From U.S. JCS, 2008)

3. Threat Environment

The threat environment that riverine forces can operate in is also constrained. As Figure 4 shows, threat environments are broken up into three levels, with level I being the least severe, and level III being the most severe.

LEVELS OF THREAT

THREAT LEVEL	EXAMPLES
LEVEL I	Agents, saboteurs, sympathizers, terrorist, civil disturbances
LEVEL II	Small tactical units, unconventional warfare forces, guerrillas, may include significant stand-off weapons threats
LEVEL III	Large tactical force operations, including airborne, heliborne, amphibious, infiltration, and major air operations

Figure 4. Levels of threat (From U.S. JCS, 2010)

As per NTTP 3-06.1 (2008), riverine forces are authorized to operate in a level I and level II threat environment only. Again, this is not prohibitive because most stability operations missions and tasks would not be utilized against a level III threat, such as a large tactical force.

D. U.S. NAVY RIVERINE—MY EXPERIENCE ON THE RIVER[4]

During his first combat patrol in Iraq, the author was speeding along Lake Qadisiyah at around 30 knots. The Navy's riverine force was not there yet in full, but a few members came ahead to patrol with the U.S Marines that were conducting the riverine mission, Dam Security Unit (DSU) Three, to learn the ins and outs of riverine operations on the Euphrates River. The mission that day was to engage the local population of the lake, mostly fisherman, and talk to them about the local happenings and things they have noticed. As the intended landing site, a small set of homes on the lakeshore, was approached, the patrol adjusted formation. One boat each took front and rear security, while the last of the three boats maneuvered to insert the Ground Combat Element (GCE), which the Riverines would call Riverine Maritime Interdiction Operations (RMIO) teams.

[4] The following is a personal account of an actual mission the author conducted on Lake Qadisiyah in Al Anbar Province, Iraq in February 2007. The purpose of this vignette is to provide a basis for comparison of what could be asked of riverine forces, as discussed above, to what current capabilities can be accomplished in the Iraqi theater of operations.

So far, everything seemed to be going as planned and trained. The riverine forces were able to maneuver fast, were very flexible in what missions were undertaken, were able to land forces ashore, and were well equipped with machine guns, grenade launchers, and small arms. Since things were seemingly going so well at the landing area (Figure 5), the author began to ask some questions.

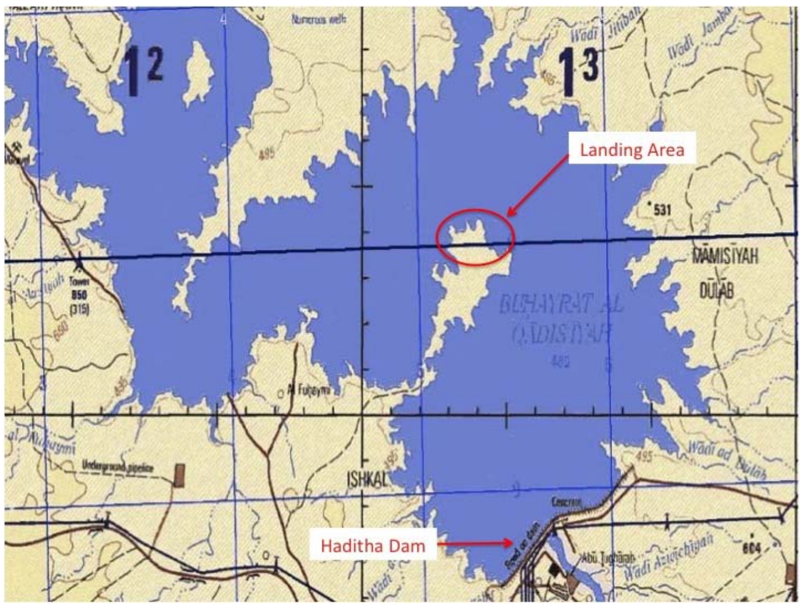

Figure 5. Lake Qadisiyah, Al Anbar Province, Iraq

When the question was asked how the headquarters (HQ) element was able to track the boats, the author was dismayed to learn that there was only one working Blue Force Tracker (BFT) on the boats, so tracking of all three boats was impossible. When boats without BFT were used, a standard 15-minute position call back was used, hardly real time. The author assumed that it would be commonplace to have air support on hand during missions, but learned that air support was rare, utilized only for large or complex missions. It was also discussed that dedicated helicopter support, when available, was limited to two to three hours, while dedicated fixed wing support was even shorter, about forty-five to seventy-five minutes. Non-dedicated support resulted in even shorter stay times. Without an ability to see beyond what could be discerned by line of sight

(LOS), the riverine force was exposed. This was showcased only a few minutes later. As the shoreline was approached and insertion began, two local males saw the boats and started walking away from the small village. They could be seen walking away, but because the DSU had to take time to set security and insert at a point that would allow positive control of the terrain, these two individuals were able to "get away" while only moving at the speed of a leisurely stroll.

Concerned that someone was escaping from the village that could have useful information, or perhaps could be a person of interest, the GCE began to question the local villagers. The Marines did not know the local language well, and neither did the Navy riverines that would be coming soon to replace them. The Marines worked off flash cards and booklets, as well as heavily relied on interpreters who were limited in availability at best. When the Marines were asked about past information that had been gathered, such as who the villagers were, who we were talking to, when the Marines were there last, what other units have talked to them, and what information they were able to provide in the past, the reply was that that information was not immediately available to them. Unfortunately, all of that information was documented in an after-action report (AAR) which was filed away back at base. It seemed unwise to be without such information that should be immediately available in order to access, analyze, cross-reference, etc. It was assumed that the Marines would at least know who these villagers were, but very few of them had IDs, and Iraqi IDs were easily forged. Those that did go through the arduous process of obtaining IDs, usually left them at home, so nothing would happen to them, especially fisherman out making their catches on the lake. This made for a very complicated and lackluster ability for the DSU to make positive identification.

Asking about what kinds of information or results usually come from these encounters, it was learned that usually either no one knew anything, or communication broke down because of the language barrier. It seemed that communication might be easier, if this process did not take as long and was not

so arduous. When asked about units in Iraq bringing soccer balls and candy along to facilitate the engagement process, the DSU replied that usually there were not enough of those types of materials to bring regularly.

As the GCE was recovered, the mission commander was informed that something interesting was found in one of the homes. They were able to recover some jihadist literature. This information is something that should be reported and transmitted to HQ right away. Unfortunately, there was no capability to send a copy for analysis. In fact, that capability did not even exist at HQ. The document would have to be walked over to the adjacent battalion, before it could be scanned and sent for analysis. It felt like there was a lost opportunity and that whatever information was on the paper, would have to be acted on days later at the soonest. As the DSU pulled away from the shore to make their way back to base, a very fast storm blew in and struck the unit. The possibility that a storm might arrive while the patrol was ongoing was not part of the mission brief. Additionally, the unit was not updated on that possibility during the mission, as real-time weather updates do not get down to the individual unit level, especially while out on patrol. That seemed dangerous and, indeed, it was. During the hour-long transit back to base, the DSU hit 6- to 8-foot waves and ended up damaging some weapons and mounts in the process, as well as suffering one personnel injury.

The above vignette provides some “real life” context to what can be found in the Joint and Navy publications. In this case specifically, the lack of technology that was available to the DSU had caused possible insurgents to escape, a loss of situational awareness with respect to the weather, and vital information in the form of the jihadist literature to be unable to be transferred to those that could provide proper analysis. The limitations discussed previously made themselves readily apparent on this mission, which proved to be typical with other missions that were conducted by riverine forces in Iraq in 2007.

E. ADDRESSING LIMITATIONS

The capabilities of the USN riverine forces are broad, and they present the joint force commander with a capable option for use in stability operations. The limitations, on the other hand, prevent the riverine forces from being a force that is consistently chosen as a necessary capability. These limitations fundamentally make the riverine force mission a more dangerous one, because the limitations in identification, situational awareness, and communication mentioned above add risk that this thesis argues is unnecessary and correctable. In the following three chapters, this thesis will make the argument for the corrections needed to reduce the risk that the riverine force is required to currently accept when conducting missions, specifically in the realm of stability operations.

THIS PAGE INTENTIONALLY LEFT BLANK

III. BIOMETRICS

A. OVERVIEW

Biometrics are a collection of technologies that enable the ability to read, store, and verify human characteristics in order to provide a positive identification. The U.S. Government Accountability Office (GAO) (2004) provides a more detailed definition:

> Biometric technologies are authentication techniques that rely on measuring and analyzing physiological or behavioral characteristics. Identifying an individual's physiological characteristic involves measuring a part of the body, such as fingertips or eye irises; identifying behavioral characteristics involves deriving data from actions, such as speech.

The reasons for collecting this information can vary, but essentially the goal is to be able to provide an ability to verify the identity of a given person by matching the collected information to a stored biometric profile. These technologies are not limited to persons that are alive, present, or cooperative only. Biometrics signatures can be obtained from persons both alive and dead, a classic example being fingerprints. Being in the same location is not required for a voice "fingerprint" or to collect fingerprints left at a location of interest such as a weapons cache. Additionally, face recognition does not require the notice or cooperation of the person being scanned. According to Verett (2006), additional ways to obtain a biometric signature include physical biometrics such as hand geometry, vein mapping, and iris recognition, as well as behavioral biometrics such as signature and keystroke recognition.

The second step of verifying an identity using biometrics is to compare the collected information against a repository of biometric signatures. This repository can be local, i.e., inside or attached to the device, or remote. The advantage of a local database is that the comparisons to existing profiles can happen much faster than by accessing a remote source. On the other hand, a local database

only has a limited amount of storage, so connecting to a remote database is ideal if there is a large range of possibilities regarding the match. Ultimately, all profiles are uploaded to the DoD Biometric Task Force (BTF) whose mission is to "lead DoD activities to program, integrate, and synchronize biometric technologies and capabilities and to operate and maintain DoD's authoritative biometric database to support the National Security Strategy (Biometrics Task Force, 2008)."

B. IMPLEMENTATION

1. Current Implementation

U.S. Navy Riverine Forces are not currently using any biometric-based capabilities. Other forces currently deployed to both Iraq and Afghanistan are using biometric systems regularly to enhance combat effectiveness. According to Jennings (2009) at the DoD Biometrics Program Management Office (PMO), the Biometric Automated Toolset (BAT) (Figure 6) and Hand-Held Interagency Identification Detection Equipment (HIIDE) (Figure 7) are the systems most widely used.

Figure 6. Biometric automated toolset (BAT) (From Jennings, 2009)

As described by the U.S. Army (USA) and U.S. Marine Corps (USMC) Counterinsurgency (COIN) Center (2009), biometrics technology "is applicable across the full spectrum of operations to achieve such effects as: stripping insurgent of his anonymity, separating insurgent from populace, enhancing force protection, and increasing confidence in host nation security forces." Because there is a multitude of advantages gained by the use of biometric technologies, the missions where these technologies are utilized vary widely. The Center for Army Lessons Learned (CALL) (2008a) describes the seven most common missions in which biometric technologies were utilized in Iraq in 2008:

- Entry control point (ECP) operations at forward operating bases (FOB)–to manage who had authorized access or been approved to work on the base.
- Population management and control operations (included census operations)–to determine who should and should not be in a given area and overall accountability.
- Local hire work programs–using HIIDE to validate workers on payday, etc.
- Raids and other kinetic operations–to find and terminate or detain predetermined targets and not unnecessarily extract others not associated with the target folder.
- Site Exploitation–to match insurgent biometrics left at blast or cache site (latent fingerprints on IED debris, etc.).
- Detainee operations supporting custody and control–supported in processing, daily accountability, and release programs.
- Actions on the objective–enrolling biometrics on personnel in event areas (IED / Explosively Formed Penetrator (EFP) blast sites, etc.) when combined with analytical processes is critical in identifying potentially involved parties.

Figure 7. Hand-Held Interagency Identification Detection Equipment (HIIDE) (From Jennings, 2009)

All of the above scenarios are likely missions that would take place within the context of stability operations. Additionally, each one of the above scenarios, with the exception of a raid, riverine forces are currently tasked with or would be expected to be able to accomplish.

2. Potential Implementation

Riverine forces would have little trouble implementing biometric systems into their Table of Allowances (TOA). To make the implementation successful, biometric systems would have to be procured and integrated at both the HQ and Detachment levels of the RIVRON. The HQ-level entity that would utilize the systems would be the N-2 (Intelligence) office. This office is responsible for intelligence collection, dissemination, and reporting, as well as in charge of detainee operations for any detainees that are brought back from riverine missions. The primary uses of these systems, according to U.S. JCS JP 3-24 (2009b), would be to obtain biometric information gathered from a detachment's missions and correlate it with any larger databases that are available to determine what information is available about the individual. Whether there

exists prior information in the database or not, the N-2 office will also have the opportunity to supplement the raw biometric information with tags. Tags such as family identities, vehicles, location obtained, time of day, language spoken, known associates, and many others provide an ability to enhance the information gained from a single biometric scan and allow the correlation of tags to find commonalities between individuals in various databases at the fusion center or above levels.

While most of the correlation of databases and tagging of data would take place at the HQ level, the initial biometric scans that make that work possible is done by the RMIO teams that are part of each detachment. Since at least a portion of the RMIO team is included as part of every mission, and they have no specific duties to attend to onboard the RPB like the boat crew does, they are the best choice for the integration of these systems. Additionally, all biometric scans will have to take place ashore, with the exception of boat-to-boat interdiction operations, so again, the RMIO team makes the most sense for the assignment of conducting scans. As JP 3-24 (2009) describes, the most important capability that must be in hand for the scans to provide value is access to a database containing past biometric scans. Both local and remote databases provide different benefits and limitations, which is mentioned above, but the most important aspect is to ensure that feedback is being passed as to whether the solution in use is meeting the needs of the RMIO in terms of scan comparison. If the location where the riverine forces are operating is largely static, then local databases will work well, as long as they are periodically updated. On the other hand, if the situation is fluid, or the operating area is large, local databases may not provide the capability to bring as big a comparison set as needed. In addition to the database situation, RMIO teams must be prepared to take biometric scans in a variety of situations, to include both persons that are cooperative or non-cooperative, alive or dead, and even situations where no person is present, such as a crime scene or a location in which a recent significant action (SIGACT) took place. It is also important for the RMIO team to take detailed notes with respect

to each scan in order to facilitate accurate and detailed tagging. This will assist the N-2 shop in accomplishing the overall goal that Woodward Jr. (2005) describes as “link an enemy combatant or similar national security threat to his previously used identities and past activities, particularly as they relate to terrorism and other crimes.”

C. BIOMETRICS IN USE

Biometric systems, as they become more prevalent throughout the U.S. military, are going to be found to be useful throughout various types of conflict and through the associated full range of that conflict. For stability operations specifically, the use of biometrics are discussed in the following three scenarios:

- Humanitarian Assistance/Disaster Relief
- Counterinsurgency
- Government and Security Force Development

1. Humanitarian Assistance/Disaster Relief

The U.S. JCS Military Support to Stabilization, Security, Transition, and Reconstruction Operations (SSTRO) Joint Operating Concept (JOC) (2006) has delineated a number of operational capabilities that apply in stability operations. While operations using biometric systems are too specific a capability to be identified in this document, the overarching capabilities that biometrics provide would be a subset and are identified in Table 2.

Objective	Capability
Deliver humanitarian assistance	The ability to manage crowds of refugees/victims
Conduct strategic communication	The ability to broadcast U.S. and coalition intentions and to help the local population find quick survival relief.

Table 2. HA/DR biometrics objectives and capabilities (From U.S. JCS, 2006)

One of the many challenges that exist in a HA/DR environment is a displaced population. The severity of the displacement can vary, but the numbers are usually staggering and hence unwieldy. For example, The Telegraph (2010) reported after the earthquake in Haiti in 2010, 400,000 Haitians were displaced from the capital of Port-au-Prince. Alternatively, according to the United Nations Children's Fund (UNICEF) (2009), after the 2004 tsunami in Indonesia, nearly half a million people were displaced, many having to resort to fleeing to other countries. In these very grave situations, biometrics can be used in multiple ways. The DoD Biometrics Identity Management Agency (BIMA) (2009) discusses this situation in the following scenario:

> The U.S. government responds to a request for help from a country that has experienced a catastrophic disaster. There is an immediate need to locate, rescue, and manage the local population. The host government authorizes the multinational response force to collect biometric samples from the civilian population to assist with the refugee management process. Identities are managed using biometrics to ensure proper distribution of food, medical attention and supplies, transportation, and the reunification of families separated during the disaster. Fraudulent distribution of humanitarian aid is reduced, and families are reunited more quickly.

An even more unfortunate result of natural disasters, and the many other reasons that may cause a HA/DR crisis, is the amount of deaths that are suffered. The tragedy extends itself when families are unable to find their loved ones or when the dead cannot be identified. The result in Haiti after the 2010 earthquake, as reported by Waterfield (2010), was that over 10,000 of the deceased were buried in mass graves every day, unidentified. Even in the face of such an unimaginable situation, biometric systems are useful. As shown in Figure 8, the biometric scanning of bodies before they are taken away for transport allows for proper identification. This primarily aids families, as they can gain some closure by knowing the fate of their loved ones. With the use of tagging as mentioned earlier, details important to the family, such as burial location, can be identified. Secondly, biometric data will allow scientists and

historians who have always debated the details of disasters to have some definitive data regarding the aftereffects. Data provided by the dead could prove important in planning for the response to future disasters, to include identifying logistical, transportation, and medical response requirements.

Figure 8. Fingerprints from a victim of the 2004 Tsunami are examined by a forensic expert in Phuket, Thailand (From Jennings & Chan, 2005)

Navy Riverine forces play a unique role in HA/DR scenarios, because they are able to access different areas that are no longer accessible due to various reasons. Waterways tend to change drastically during weather-induced disasters such as typhoons or floods. This change presents an unplanned challenge to conventional land-operated forces, as they are forced to plan around new water obstacles. Riverine forces are in just the opposite position: they can use these newly formed, and likely temporary, waterways to gain access to terrain they previously did not have access to. With regard to other disasters, such as earthquakes or tornados, many times the waterway may be fouled by debris, sunken vessels, etc. The shallow draft of riverine craft allow mostly unimpeded

access to these fouled areas that conventional water craft would be unable to operate in unrestrained, due to potential danger to the vessel.

Both the newly accessible areas and the unimpeded access to fouled areas give riverine forces the advantage of population access, which is key to biometric operations. This enhanced access allows riverine forces to collect biometric data from populations that are inaccessible to other units (Figure 9). While biometric collection is likely to be a secondary mission to one of search and rescue and displaced persons management, it is a mission that can easily be conducted concurrently with minimal primary mission disruption.

Figure 9. Displaced persons gather along a waterway after the 2010 Haiti earthquake (From McNamee, 2010)

2. Counterinsurgency

As was the case with HA/DR, biometrics support to stability operations is too specific of a capability to be delineated in detail in the Military Support to SSTRO JOC. Also like HA/DR, there are objectives and capabilities, shown in Table 3, that enable operations in which biometric systems will play a key role.

Objective	Capability
Establish responsive battlespace awareness / understanding	The ability to tag, track, and localize hostile elements in all domains.
Establish and maintain a safe, secure environment	The ability to use both kinetic and non-kinetic means to capture and defeat terrorists/insurgents, often in dense urban environments, while minimizing collateral damage.

Table 3. Counterinsurgency biometrics objectives and capabilities (From U.S. JCS, 2006)

One of the most basic tasks any combat unit has in a counterinsurgency environment is to go on patrol and immerse themselves amongst what is almost always the center of gravity, the people. When units are able to spend time among the people as shown in Figure 10, the opportunity presents itself to gain an understanding of their concerns, issues, motivations, habits, and many other things. According to the COIN Center (2009), using biometric systems to enhance this interaction "can provide units with a better understanding of the populace in their areas of operations, which can guide operations to better secure that populace."

Figure 10. A U.S. Marine hands a local Afghan in Marja a free radio after inputting his data into the BAT system (From Hunt, 2010)

Operations that are conducted at the tactical level can have very far-reaching effects. As discussed in the USA/USMC Counterinsurgency Center SITREP (2009) and mentioned above, using biometric systems as identity verification tools "is applicable across the full spectrum of operations to achieve such effects as: stripping insurgent of his anonymity, separating insurgent from populace, enhancing force protection, and increasing confidence in host nation security forces." Specifically, Hom (2008) describes how these effects can be achieved. He says that biometric systems utilized throughout the area of operations "would allow for identification of individuals at any node in the network as well as tracking of 'tagged' persons as they move through the network. Thus, the time and space in which insurgents can exist and move undetected would shrink significantly."

An even more specialized set of capabilities that have become required skill sets for tactical level units is Tactical Site Exploitation (TSE), sometimes also called Sensitive Site Exploitation (SSE). The Center for Army Lessons Learned (CALL) (2008b) defines TSE as "the action taken to ensure that documents,

material, and personnel are identified, collected, protected, and evaluated in order to facilitate follow-on actions. TSE focuses on the actions taken by soldiers and leaders at the point of initial contact." There are two fundamental ways in which the use of biometric systems can make a TSE more productive and informative. First, the TSE team will run scans on the personnel that give interviews about what happened at the site, or those that were involved or injured at the site. This information allows these individuals to be linked or "tagged" to the site, which will aid in future analysis. Even more advantageous is if one of these individuals scanned, were actually involved in a previous criminal/insurgent act, which could warrant their immediate detention. The second way a TSE team can successfully utilize biometrics is by gathering latent biometrics signatures such as fingerprints from items at the site. Some of this information can be gathered on the scene, but some will be required to be sent to a lab, in which further testing and data gathering can be done for further biometric exploitation for information such as DNA.

Riverine forces have a unique capability to utilize biometrics in a counter-insurgency environment. As mentioned above, conducting patrols is the essential ingredient to learning the fundamental understanding about how the population operates and conducts themselves. Riverine forces have the unique ability to patrol along a travel and economic pathway that few other units can, the waterways. This allows riverines to have sole access to the population that travels and trades along the routes afforded by the waterways. The waterway is an essential element of the "human terrain." With riverine forces operating and collecting biometric data in these locations, the data can connect persons who would otherwise be considered disparate, making analysis much easier and more comprehensive. Hom (2008) argues this point as he says to make "biometric profiling and tracking ubiquitous," there must be "adequate resources" to cover the extent of the operating area, which for many parts of the world, include waterways, making riverine forces the crucial capability to fill the gap that would otherwise exist. Additionally, as the waterways are unlikely to be as well

secured through the use of checkpoints and crossings like roadways will, these routes of travel offer a more enticing path for those wishing to not be detected by the more numerous land forces. This access to the terrain, both physical and human, that other forces have difficulty accessing, also allows for TSE to be conducted by riverine forces in the locations. The key capability that riverine forces offer is not only being able to conduct TSE on locations they identify or are tasked with, but also to assist other units. Many ground units may not travel with a TSE capability, and for those operating near waterways, riverine forces many times are able to assist adjacent units by conducting TSE, while security is set and maintained by the ground unit.

3. Government and Security Force Development

A unit conducting stability operations is likely to have to conduct government and security force development. According to the U.S. JCS Military Support to SSTRO Joint Operating Concept (JOC) (2006), there are two required operational capabilities where the use of biometric systems would be a force multiplier when conducting this type of development (Table 4).

Objective	Capability
Establish a representative, effective government and the rule of law	The ability to assist in the organization and training of personnel to work in the various government ministries and agencies.
Establish and maintain a safe, secure environment	The ability for the U.S. Armed Forces to train, equip, and advise large number of foreign forces in the full range of SSTR-related skills.

Table 4. Government and security force development biometrics objectives and capabilities (From U.S. JCS, 2006)

Government development is a challenge that requires a two-pronged approach. First, there must be steady advances in the capacity and capability of the government in the tasks that they, and the United States or coalition force are trying to accomplish. At the same time, the population must be gaining confidence in the government's ability to do these tasks. The use of biometric systems can provide a technical capability that works hand-in-hand with the knowledge and experience capabilities that are being concurrently developed. There are many different functions that the government executes, that will be greatly enhanced by the use of biometrics that include identification card issue and verification, background checks, voting, and the conducting of a census. As described by the USA/USMC COIN Center (2009), the underlying capability that makes the ability to conduct all of the above functions properly, is a centralized biometric database that the government can use to input and verify biometric signatures. Hom (2008) makes it clear that the result of a central biometric database and a government that is executing their inherent functions in a dependable and reliable manner is "stability."

Like government development, security force development requires the same two-pronged approach of not only competency of operations and functions, but of confidence of the population as well. In general, the security forces can be examined in two separate, but very similar ways, the internal or population security forces, made up of the police, and the external or national security forces, which consist of the armed forces with a land, air, and maritime component. While the overall mission of these organizations can vary widely, fundamentally they must do many of the same things, such as recruit, train, retain forces, detain criminals or opposition forces, and enforce access to locations such as roads, bases, buildings, airports, ports of entry, etc. These functions lend themselves very well to the leveraging of biometric systems to make them more capable at conducting these missions in an accurate manner. As the CALL (2008a) describes, the use of biometrics in Iraq has been very effective at ensuring that police candidates are fully vetted before being brought

into the police force. In Afghanistan, the pre-vetting of police and army personnel plays a large role in both preventing and resolving problems with retention. Any force member who decides to abandon their position knows that any time in the future that they are subjected to a biometric scan, they would be identified immediately, resulting in their detention, and with their absence being resolved by their original unit, once they are returned.

Riverine forces are uniquely able to assist in both government and security force development. As mentioned above, the riverine's access to terrain inaccessible by conventional forces is one of the most advantageous reasons such a role is needed. In this case though, it is not the riverine force's role to conduct the functions and activities themselves, but training and assisting the government and security forces on how best to execute. As Paquin (2009) states, this has already been successful during the U.S. Naval Mission in Colombia in which the Colombian Navy and Colombian Coast Guard have received extensive training on maritime interdiction and law enforcement. Specific to the biometric system capabilities the government would be looking to be utilized as mentioned above, the leveraging of riverine forces would be an excellent way to provide government services to those that use the waterways as their main thoroughfare, and may not have the needed access to the main city centers where most government services are offered. Additionally, any maritime specific government services, such as boat or fishing licensing, would be greatly enhanced by riverine force access. On the security force development front, there is always a need to maintain security on the waterways, especially as it can act as a main thoroughfare for those wishing to avoid traditional roadway checkpoints. Additionally, trafficking of illegal drugs, weapons, or persons is very likely to happen along a waterway. Training the security force, as shown in Figure 11, that would conduct the enforcement of laws on the waterways, and in the process of enforcing these laws utilizing biometrics to enhance their capability to do so, is a prime example of where riverine force use provides a unit that is able to conduct the mission where many others cannot.

Figure 11. An Iraqi Solider assigned to Iraqi Riverine Police Force during special boat maneuvers and weapon handling training (From Aho, 2006)

D. CONCLUSION

The use of biometric systems has extensive capabilities that can be used in a variety of situations that are likely to present themselves in the near future, as the United States takes on larger stability operations missions. The capabilities gained by the implementation and use of this specific set of systems is significant, from a cost perspective, when compared with costs associated with major weapons platforms. The most important part of the use of biometric systems is that it gives you more information on which to base decisions.

In the next chapter, we will discuss the various ways riverine forces can leverage unmanned platforms in support of stability operations to achieve situational awareness over the battlefield, facilitate command and control, and collect data for analysis.

IV. UNMANNED SYSTEMS

A. OVERVIEW

An unmanned system is a broad term that encompasses many different types of systems. The most prevalent in the U.S. military currently are the Unmanned Aircraft System (UAS), Unmanned Ground Vehicle (UGV), and Unmanned Maritime System (UMS). UMS is made up of both Unmanned Undersea Vehicles (UUV) and Unmanned Surface Vehicles (USV). According to the Office of the Secretary of Defense (OSD) (2005), what makes unmanned systems advantageous is that they specialize in the “dull, dirty, and dangerous.” Dull tasks are those that require lengthy on-station time or a constant state of alertness. Those tasks that are dirty are ones in which it might be politically sensitive to send in manned vehicles, or might require sampling of hazardous materials. Lastly, dangerous tasks also include those associated where a potential loss of life is high, like extended hostile action or flying into a hurricane.

The increasing requirements for intelligence, surveillance, and reconnaissance (ISR) include the incorporation of numerous sensors. Unmanned systems are becoming more widespread, as the traditional missions of manned scouting and reconnaissance have been unable to keep pace with the information demands of commanders. As stated in the OSD (2005) Unmanned Aircraft Systems Roadmap: “The dominant requirement for sensing is for:

1. Imaging (visible, infrared, and radar)
2. Signals (for the Signals Intelligence (SIGINT) and Suppression of Enemy Air Defenses (SEAD) missions)
3. Weapons of Mass Destruction (WMD) (chemical, biological, radiological [CBR])
4. Meteorological and Oceanographic (METOC)
5. Magnetic (anti-submarine warfare (ASW) and mine countermeasures [MCM])”

In recent years, the use of unmanned systems has been expanded to include missions conducting offensive operations. Although this is a proven capability that will continue to become ubiquitous in unmanned systems, it will not be discussed as part of this thesis.

The use of unmanned systems follows a predictable path of the following steps:

1. Launch
2. Operation and Collection
3. Recovery

The logistics of launching and recovery are very important, especially for riverine operations. The remainder of this chapter will focus mostly on collection and the missions in which specific collection goals are laid out, but the challenges associated with launching and recovery should not be forsaken.

B. IMPLEMENTATION

1. Current Implementation

When the U.S. Navy stood up Riverine Group One and active riverine squadrons were also commissioned in 2006, unmanned systems were a capability that was integrated in planning, but training, logistics, and exercising were not existent during pre-deployment preparations, limiting their success. The extent of the unmanned systems that were fielded only consisted of one type of UAS, the Silver Fox, with no UGV or UMS on the horizon. While the Silver Fox UAS, as shown in Figure 12, had potential, there were two fundamental problems: First, the squadron had difficulty integrating UAS operations with boat operations during the training cycle for deployment. As Captain Michael Jordan, the Commodore for Riverine Group One, described, “We have a few folks trained to use them, but we need to get better at that. It’s a key asset we need to be utilizing better (Faram, 2008).” The second problem was a reduction of the effective range due to electromagnetic interference in the operating area, which was discovered by RIVRON 1 after multiple vehicles were lost. Due to the

numerous amounts of electromagnetic countermeasures used to combat the IED threat in theater, there exists a significant amount of electronic pollution. As Hodge (2009) from Wired reported, Commander William Guarini, Commanding Officer of Riverine Squadron One, described the Silver Fox as “very susceptible” to this interference. This same problem presented itself when operating in vicinity of the Haditha Dam in Iraq, with the dam producing its own electromagnetic interference, causing the same effect on the drone.

Figure 12. Silver Fox UAS (From Office of Naval Research, 2009)

While there were other UAS in consideration, to include the Wasp UAS, to supplement or replace the plagued Silver Fox platform, Wilson (2009), from the Office of the Chief of Naval Operations (OPNAV) N851, concluded that NECC would wait for the Small Tactical Unmanned Aircraft System (STUAS) Tier II to become available. This will take some time though, as it was recently announced by Naval Air Systems Command (NAVAIR) (2010) on July 29, 2010 that the contract for STUAS Tier II was awarded to Insitu Incorporated. Insitu (2010) announced following the award that Initial Operational Capability (IOC) is expected by the fourth quarter of Fiscal Year (FY) 2013.

Riverine forces, of course, have not been alone in the quest to expand capability by utilizing unmanned systems. In fact, in Table 5, the FY 2009–2034

Unmanned System Integrated Roadmap describes the numerous different unmanned systems that are filling the requirements of nine specific Joint Capability Areas[5] (JCA).

Unmanned Systems by JCA and Domain Numbers of Named Systems					
Battlespace Awareness	**84**	**Corporate Management & Support**	**1**	**Logistics**	**28**
▪ Air	30	▪ Air	0	▪ Air	6
▪ Ground	38	▪ Ground	1	▪ Ground	22
▪ Maritime	16	▪ Maritime	0	▪ Maritime	0
Building Partnerships	**32**	**Force Application**	**42**	**Net-Centric**	**18**
▪ Air	6	▪ Air	22	▪ Air	8
▪ Ground	18	▪ Ground	10	▪ Ground	10
▪ Maritime	8	▪ Maritime	10	▪ Maritime	0
Command & Control	**20**	**Force Support**	**20**	**Protection**	**66**
▪ Air	8	▪ Air	2	▪ Air	11
▪ Ground	12	▪ Ground	18	▪ Ground	42
▪ Maritime	0	▪ Maritime	0	▪ Maritime	13

Table 5. Density of named systems within each JCA (From OSD, 2009)

In JP 3-24, the U.S. JCS (2009b) argues passionately for unmanned systems, saying their use strengthens local intelligence, enhances regional and national reporting, and bolsters operations at all levels." Because there are a multitude of advantages gained by the use of unmanned systems, the missions where they are utilized vary widely. The following, from OSD (2005), is a list of the top fifteen missions for ISR assets ranked by importance by Combatant Commanders and Service Chiefs in 2004:

1. Reconnaissance
2. Precision Target Location and Designation
3. Signals Intel
4. Communications/Data Relay
5. Battle Management
6. Chem/Bio Reconnaissance
7. Counter Cam/Con/Deception
8. Combat SAR

[5] Joint Capability Areas (JCA) are collections of like DoD capabilities functionally grouped to support capability analysis, strategy development, investment decision making, capability portfolio management, and capabilities-based force development and operational planning (OSD, 2009).

9. Weaponization/Strike
10. Electronic Warfare
11. Information Warfare
12. Mine Detection/CM
13. Digital Mapping
14. Covert Sensor Insertion
15. SOF Team Resupply

All of the above missions are likely to take place within the context of stability operations. Additionally, each one of the above missions, with the exception of a battle management and strike, riverine forces are currently tasked with, or would be expected to be able to accomplish, at least in a limited manner.

2. Potential Implementation

The use of unmanned systems as part of the Navy Riverine Forces was planned from its inception. As reported by *Signal* (Ackerman, 2007), Captain Dave Balk, the assistant chief of staff for strategy and new technology at the Naval Expeditionary Combat Command (NECC) said, “the goal is a three-dimensional unmanned vehicle presence that employs aerial, surface and underwater vehicles to improve riverine situational awareness.” To make this goal a reality for today’s forces, specific integration must be addressed.

For unmanned systems to be successful in RIVRONs, they must be integrated into both the HQ and detachment sections of the squadron. The squadron personnel that are assigned as unmanned system operators will need to work closely with both the intelligence (N-2) and operations (N-3) portions of the headquarters element. For most seamless employment, they should be assigned to the operations section to ensue that their use was based on operational need. One reason that unmanned system detachments have not been entirely successful is because the personnel making up the detachment are still completing training and schools at the same time as the boat crews and RMIO teams. The remaining time between training schools and deployment does not provide an adequate opportunity for squadron or detachment personnel

to integrate, train, and rehearse employment tactics to the point where the integration of assets; boats, personnel and unmanned systems becomes seamless.

While the operations department handles tactical employment of the unmanned system detachment within boat detachments, the N-2 (Intelligence) department is responsible for the collection and analysis of the data captured. While any data captured by the unmanned system is immensely helpful during operations on the ground, many times the most useful data is found when analysis is done after operations are complete. This time allows for the intelligence specialists assigned to the N-2 office to catalog, tag, assess, and report on what data was captured by the unmanned system. This reporting is crucial, as it allows key data to be shared with adjacent units that operate in the same area as well as up to higher echelon intelligence organizations such as fusion cells.

For actual operations, the unmanned systems detachment must be assigned to a riverine boat detachment. This ensures UAS planning is conducted in conjunction with the squadron N-3. During operations, the unmanned systems detachment would be under tactical control of the Officer in Charge (OIC). Any specific requests for information (RFI) would be incorporated into the pre-mission planning and therefore become an integral part of the operation.

The missions for which unmanned systems are sought are expansive. As Russo (2006) describes, "in riverine operations, one of the keys to success is having as much situational awareness as possible." While there may be numerous other missions the riverine forces will actively use unmanned systems for, situational awareness will be a major part of each mission and the primary tasking for all unmanned systems. Similarly, Spangler (1995) portrays dedicated helicopter support in support of riverine operations during the Vietnam conflict, as the same capability unmanned systems can provide to increase "ambush resistance, airborne observation, and early warning." This capability is especially

important when riverine forces have placed RMIO teams ashore. Having unmanned systems available, especially UAS in this case, allows RMIO teams to be forewarned of enemy activity and potential ambush sites, as well as allowing them to much more easily identify helicopter landing zones (HLZ) in case a MEDEVAC is necessary or spot alternate extraction points along the river in case emergency extraction is needed.

One often-overlooked portion of riverine operations is the waterborne guard post (WBGP). As depicted by the Riverine Operations NTTP (U.S. DON, 2008), the WBGP is how riverine forces conduct static surveillance. The purpose of a WBGP is for the riverine force to be still and as hidden as much as possible to prevent them from being seen. While the WBGP has its advantages, not being able to transit the waterway limits the field of view drastically. The use of unmanned systems in conjunction with a WBGP allows the riverine forces to multiply the amount of terrain they are able to monitor while remaining undetected. The WBGP and bivouacking, i.e., staying in a temporary camp in an unsheltered area, are also two instances where riverine forces are vulnerable to attack. Riverine forces will need to bivouac away from their base of operations as mission requirements require, and having an unmanned systems provide security over-watch can mitigate risk by providing an effective layer of security to prevent an ambush.

C. UNMANNED SYSTEMS IN USE

Unmanned systems, as they become more prevalent throughout the U.S. military, are going to be found to be useful throughout various types of conflict and through the associated full range of that conflict. For stability operations specifically, the use of unmanned systems are discussed in the following three scenarios:

- Humanitarian Assistance/Disaster Relief
- Counterinsurgency
- Government and Security Force Development

1. Humanitarian Assistance/Disaster Relief

Functional and operational capabilities that apply in stability operations are described in the DoD Military Support to Stabilization, Security, Transition, and Reconstruction Operations (SSTRO) Joint Operating Concept (JOC). While this document does not discuss unmanned systems specifically, the capabilities required for stability operations, shown in Table 6, include unmanned systems as they would play a large role in improving the overall effectiveness of the operation.

Objective	Capability
Deliver humanitarian assistance	The ability to coordinate and integrate with U.S. government (USG) agencies and multinational organizations in order to support humanitarian assistance and disaster response efforts.
Establish responsive battlespace awareness / understanding	The ability to conduct persistent surveillance of critical enemy activities in difficult and denied areas by using sensors to capture timely, relevant, and interoperable source data.[6]

Table 6. HA/DR unmanned systems objectives and capabilities (From U.S. JCS, 2006)

One of the many challenges that HA/DR missions present is that getting access to locations where initial aid and assistance, such as search and rescue, where it is needed can be very difficult. Even more challenging, is finding out where the focus of effort needs to be without area access, which can make the first steps in the execution of HA/DR operations unsure or misguided. The

[6] In HA/DR, this persistence surveillance would not be limited to only enemy activities, but expanded to all critical activities.

author observed this first hand during the HA/DR operations following Hurricane Katrina's landfall in New Orleans, Louisiana in 2005 (Figure 13).

> Even though forces had been on site for many days prior to the author's arrival on USS TORTUGA eight days after the storm, on the first day of operations there were over fifty people that were in very apparent need of rescue that had not been reached because there was no access to the 9th ward of New Orleans at that time due to flooding and road damage.

Unmanned systems are able to play crucial roles in HA/DR situations like the one mentioned. Instead of only operating where it was apparent that accessibility was possible, by using the sensors of unmanned assets, it would be possible to precisely direct operations to where recovery assets are needed most. Also crucial to effective HA/DR is quickly determining what additional assets are needed to facilitate the response. Unmanned assets can quickly provide significant details regarding various different aspects of the same event, providing valued situational awareness to the responding entity, while at the same time, as Duhan (2005) describes, reducing the number of manned aircraft needed for ISR missions, freeing them for other missions such as search and rescue.

Figure 13. Mark Scovill, Commanding Officer, USS TORTUGA (LSD-46) surveys the extent of flooding in the 9th Ward, New Orleans, LA, after Hurricane Katrina (From Watkins, 2005)

An additional challenge that poses itself during HA/DR operations is assessing the condition of the affected area. This is vitally important for response organizations to know, as gaining a comprehensive understanding of the various roadways, waterways, bridges, ports, airfields, etc. will facilitate a much greater speed of response. Ryan (2007) explains that organizations that respond to HA/DR scenarios are likely to be more mobile. These more mobile organizations are going to be able to deploy personnel and equipment to disaster zones much more quickly than in previous HA/DR scenarios. To facilitate their much more expedient arrival and provide them the information they need to get their assets into the field more quickly, the use of unmanned systems is an obvious choice. The U.S. JCS (2008) argues that utilizing ISR assets in this way "decreases risk and allows the commander more control over the timing and tempo of operations." The importance of understanding the environment to facilitate effective timing and tempo of operations was put onto display clearly after the earthquake in Haiti in 2010. As Snow, Harris, and Adhikari from ABC

News (2010) reported, there was a massive back-up of relief supplies stuck at the airport with little understanding of where or why the bottlenecks were taking place, while meanwhile millions of desperate Haitians suffered without. Using unmanned systems in this instance could have provided the data needed to map, track, and understand the movements of supplies, allowing the response forces to direct assets to correcting the bottlenecks and getting aid to those that needed it most.

Using riverine forces equipped with an unmanned system capability would be a significant step forward in gaining tactical situational awareness when executing a HA/DR operation. Riverine forces' ability to maneuver along the waterways, where no infrastructure is needed, allows them to be a first on the scene type of unit. This early access to a disaster area with unmanned systems capability gives the scene commander an early assessment as to where the focus of operations needs to be and what further assets are needed to complete those operations. Being able to provide ISR data gathered by riverine forces gives the commander an immediate advantage in developing the strategic plan for the military forces assisting in the HA/DR operations.

2. Counterinsurgency

Both functional and operational capabilities needed in a counterinsurgency environment are discussed in detail in the DoD Military Support to SSTRO JOC (2006). While unmanned systems are not specifically broken out, there are specific capabilities, shown in Table 7, in which unmanned systems could play a significant role.

Objective	Capability
Establish responsive battlespace awareness / understanding	The ability to conduct persistent surveillance of critical enemy activities in difficult and denied areas by using sensors to capture timely, relevant, and interoperable source data
Establish and maintain a safe, secure environment	The ability to use both kinetic and non-kinetic means to capture and defeat terrorists/insurgents, often in dense urban environments, while minimizing collateral damage.

Table 7. Counterinsurgency unmanned systems objectives and capabilities (From U.S. JCS, 2006)

Counterinsurgency is defined by the JCS (2001) as “those political, economic, military, paramilitary, psychological, and civic actions taken by a government to defeat an insurgency.” Fundamentally, counterinsurgency is a battle for the support of the people. The population is so important because as Tomes (2004) depicts, something as simple as having consistent engagement with the population and “anticipating problems and proactively addressing them leaves the insurgent without causes to exploit.” Critical to winning this support of the people is being able to operate outside of large bases and protected areas. As Cohen, Crane, Horvath, and Nagl (2006) describe, this highlights one of the many paradoxes of counterinsurgency that “the more you protect your force, the less secure you are.” Stavroulakis (2006) lays out that to be able to venture out of these zones of protection and be effective at the assigned counterinsurgency mission, “maximum situational awareness” is one of many essential goals. Situational awareness not only allows you to have a greater ability to protect yourself while conducting combat missions, it also provides the information needed to conduct offensive operations. Unmanned systems present a

capability that is a force multiplier in support of all of these objectives. Unmanned systems' primary mission is ISR by definition, which can be used both defensively and offensively. Defensively, unmanned systems allow for a greater understanding of the operational area and can be instrumental to formulating a common operational picture, one of the key pieces of information needed to prevent fratricide or "blue-on-blue" engagements. Offensively, (unarmed) unmanned systems can provide four of the five pieces of necessary information needed for successful target engagement as part of the "Kill Chain" presented in Figure 14 by Beaver, Mercado, Bucher, Free, Byers, and Oliveria (2006).

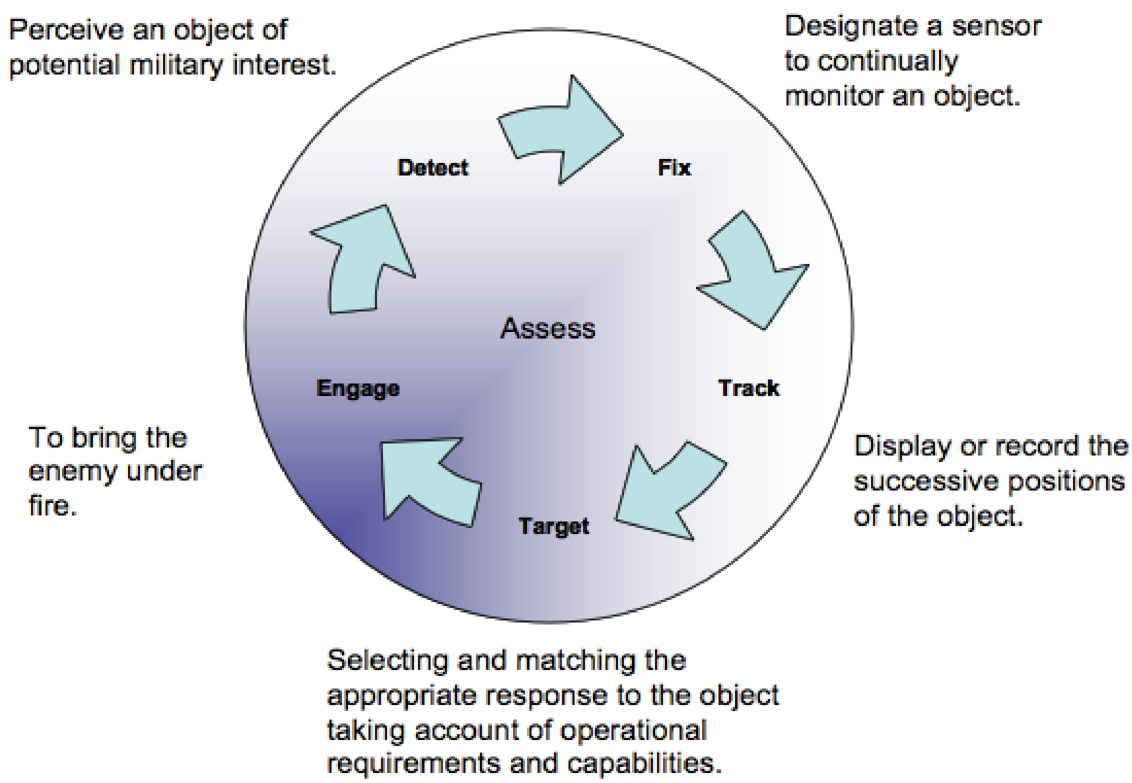

Figure 14. Functional Flow of the Kill Chain (From Beaver et al., 2006)

Another challenge in a counterinsurgency environment is that insurgents tend to blend in with the people, making distinguishing friend and foe more difficult. This is a very difficult challenge to overcome and as Cassidy (2004) says: "It underscores the importance of aggressive patrolling, population security,

and the denial of sanctuary to the insurgents." Preventing insurgents from having a sanctuary to conduct their own operations means that they must not feel comfortable enough to conduct their operations "in plain sight." As the situation for the counterinsurgent improves, the ability for the insurgent to operate with impunity decreases, requiring a much more comprehensive and ubiquitous presence of ISR. Unmanned systems present the opportunity to gain this increase in ISR capability, while allowing combat forces to focus on population-centered operations. Additionally, due to the ability for unmanned systems to stay on station for long periods of time beyond what conventional combat forces could accomplish, they are ideal, as Flynn, Pottinger, and Batchelor (2010) suggest, to be "tasked with scanning the countryside around the clock in the hope of spotting insurgents burying bombs or setting up ambushes." While single events such as these can give the counterinsurgent forces a specific location to avoid or to prosecute, sometimes more advantageous information is gained by the long-term tracking and collection of insurgent activities. As the author observed in Iraq, "regional level UAS were very successful in providing information regarding insurgent activity times, locations, and paths, allowing for the development of an intelligence picture that could be exploited at the most opportune moment." This type of long-term presence and data collections could not be accomplished by manned assets without orders of magnitude more cost and resources compared to the utilization of unmanned assets.

Riverine forces have already proven themselves in counterinsurgency conflict both in Vietnam and Iraq, and with the addition of an effective unmanned systems capability; they make themselves an even more effective force. Having the additional situational awareness that unmanned systems provide allows riverine forces to operate more often and for longer periods of time, thus drastically increasing the amount of time they can spend interacting with the populace. Unmanned systems are not only useful indentifying possible insurgent activity that may pose a risk, but, as Benbow et al. (2006) lays out, they are also useful in identifying water-borne IED threats, which pose as much of a hazard to

riverine forces as they do to the population that uses the waterway for commerce. There is no questioning that the riverine operational area is dynamic, where water, land, and air units all intermix. As Spangler (1995) identified, to be successful in this environment requires “close coordination and integration of all assets.” He argues that riverine forces needs “high tech sensors,” which unmanned systems can provide. Stolzenburg (2008) expounds on the use of sensors during OIF where riverine forces took positions to provide overwatch on avenues of approach that could be used by insurgents to disrupt ongoing operations. Coupling these routine operations with unmanned systems would give both the riverine forces and the adjacent units they are protecting much more forewarning of possible insurgent activity, preventing surprise, and in some scenarios, facilitating counterattacks to take place.

3. Government and Security Force Development

The task of government and security force development plays a key role in stability operations. Unmanned systems can assist in this development and foster legitimacy in the process. The DoD Military Support to SSTRO Joint Operating Concept (JOC) (2006) lays out operational capabilities in which unmanned systems would play a role in development (Table 8).

Objective	Capability
Establish a representative, effective government and the rule of law	The ability to assist in the organization and training of personnel to work in the various government ministries and agencies.
Establish and maintain a safe, secure environment	The ability for the U.S. Armed Forces to train, equip, and advise large number of foreign forces in the full range of SSTR-related skills.

Table 8. Government and security force development unmanned systems objectives and capabilities (From U.S. JCS, 2006)

For the people of a nation to believe in their government, they must see their presence and feel like the government is providing a service, fostering legitimacy in the process. For budding governments to which the United States is providing support during stability operations, this can be an uphill task. But, as Flynn et al. (2010) describe, "governance, development, and local populations [are] all topics that must be understood in order to prevail." There are key opportunities for success as government personnel have the opportunity to visit local communities to conduct project assessments and meet with local leaders. These local leaders will have a comprehensive understanding of what the government can and cannot do to help their community. One issue that arises is that as more engagement and fact-finding is done on the ground, this new information only creates significantly more work for the government. This is where unmanned systems can play a role; governments can collect for example air quality testing, crop data analysis (Figure 15), analysis of road and traffic conditions, etc.; utilizing unmanned assets provides an opportunity for government officials to spend more time with community leaders instead of out gathering data. As annotated in the Quadrennial Defense Review (QDR) (Rumsfeld, 2006), these unmanned systems can provide a crucial capability to the government to include "automation, integration, analysis, and distribution of information," all keys to effective governance in the 21st century.

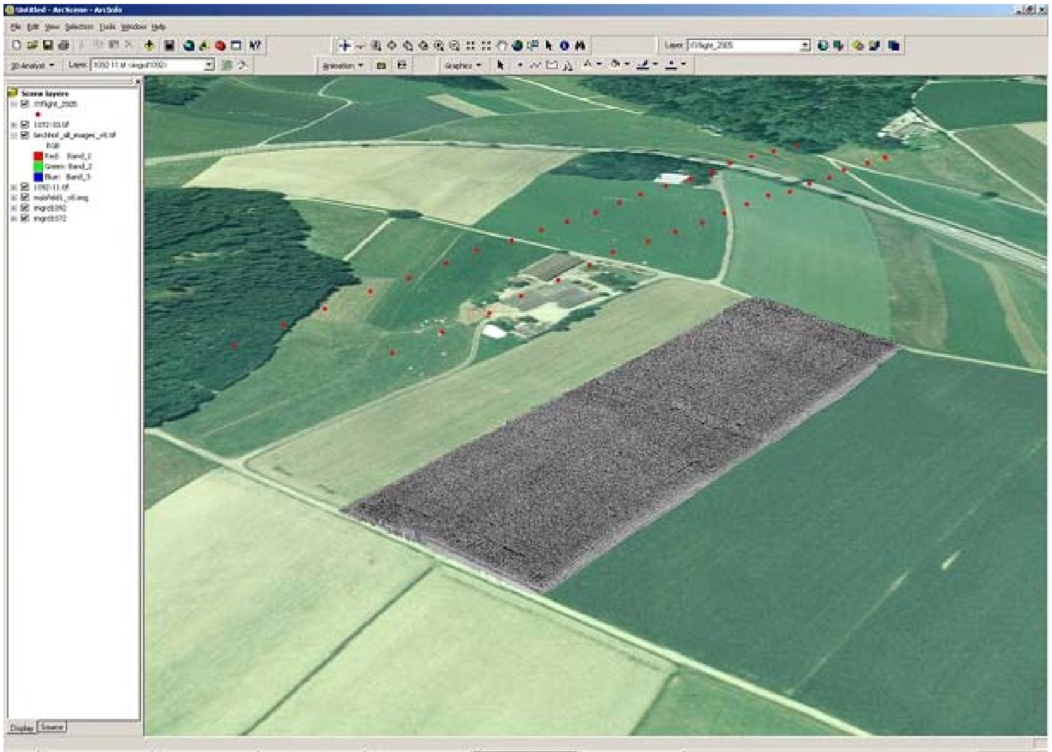

Figure 15. Crop Analysis with imagery provided by UAV (From Volger, 2006)

To enable the government growth in both capability and capacity requires a security situation that is conducive. To create this environment of security and enable the possibility of economic and societal growth is why in the QDR, Rumsfeld (2006) argues for a strong capability for countries to be "policing themselves." This does not happen automatically though, and hence is why security force development is such an integral part of stability operations. The key to successful security force operations is an innate understanding of the normal conditions of the area of operations, and what Freitas and Treadway (1994) describe as "vital information." Such information that U.S. forces can pass on to growing local security forces that can grow this understanding are an identification and analysis of actions taking place in prohibited areas, unauthorized times, or differing from normal patterns. While these tasks seem simple enough, having enough security forces on the ground to accomplish an ubiquitous understanding is challenging, especially in a stability operations

environment where the focus is likely on growth. Hedderly (2008) argues that the addition of advanced technologies can ease the “manpower burden” that would naturally exist in this situation. To accomplish these ends, the equipping of security forces that are being trained and professionalized with unmanned systems would provide an immediate capability that would make up for any personnel shortage that may exist, while at the same time, providing information that can be appropriately stored, cataloged, and mined to accomplish a greater understanding of the operating environment. Ferebee (2009) argues this quite succinctly:

> The ability to tag and track personnel and vessels regardless of size and location will greatly enhance situational awareness for everyone. Not only does electronic tracking offer increased security for personnel, it alleviates the need to exhaust resources for simple monitoring activities and provides the ability to coordinate interception efforts.

Riverine forces, equipped with unmanned systems, could provide an excellent opportunity to execute government and security force development missions. As mentioned, government presence is the first step to legitimacy as it grows. General Speer (2002) argues that like during operations in Colombia, riverine forces providing assistance on developing a government presence along the waterways allows the “government to exercise sovereignty throughout the vast regions where other governmental entities are otherwise absent.” These areas where riverine forces can provide capability coincide with the areas where government presence is needed. Opportunities for riverine forces to offer assistance in government development by way of unmanned systems include, assessing waterway conditions for fishing or building of ports, investigating dam or irrigation infrastructure, and many others. Related to security force development missions, using riverine forces would be at even more of an advantage. The instructing of foreign waterborne forces has been a staple mission of the riverine force for decades argues Paquin (2009), especially in Colombia. LaFranchi (2001) lays out that when waterways make up such an

important part of a country's lifeblood of travel and commerce, "officials see controlling inland waterways as tantamount to establishing an orderly state presence in large swatches of the country." Crucial to security forces being as effective as possible at understanding and controlling the waterways are the ability to expand situational awareness, especially air platforms. As JP 3-24 (U.S. JCS, 2009b) describes: "Airpower capability is a catalyst for government legitimacy, projecting national sovereignty, and accelerating the nation's overall internal stability as well as regional security." While airpower historically has never been started with unmanned systems, there is no reason that unmanned systems cannot be leveraged to build the beginning of an airpower capability. JP 3-24 goes on to argue that one mission for maritime security forces is to "introduce or expand existing maritime domain awareness efforts" and additional missions "may include fishery patrols, interior security, port authority, customs, and immigration." For each of these maritime domain missions, a riverine force, providing security assistance and equipped with advanced unmanned systems technology, would multiply the return on investment through expanded capability.

D. CONCLUSION

The integration of unmanned systems into the USN Riverine Force is a much easier task since it has already been attempted. The Silver Fox UAS was a noble attempt to expand riverine force capability at the onset, but now the lessons learned from the experiment need to be applied with the forthcoming Small Tactical Unmanned Aircraft System as well as the other non-aerial unmanned systems that should follow. The unmanned systems comprised of UAS, UMS, and UUV, if implemented, would play a key role in the stability operations. Future riverine forces will need to support the realms of ISR, situational awareness, persistent tracking, as well as battlefield coordination that are all made possible by unmanned systems.

In this chapter, we discussed how unmanned systems detailed to riverine forces could gather immense amounts of information that could be used by

various stakeholders to accomplish the plethora of missions that stability operations demand. Chapter V will break ground on the topic of information sharing. Information sharing is the key to making the data gathered by biometric systems, unmanned systems, or any other advanced information gathering technology work for the joint force commander, by making the data available in a timely and targeted fashion.

V. INFORMATION SHARING SYSTEMS

A. OVERVIEW

Information sharing is how modern forces are able to enhance their decision making at all levels. As one would expect, better decisions are consistently made when those who need it receive more accurate and timely information. The DoD (2007) defines information sharing as:

> Making information available to participants (people, processes, or systems). Information sharing includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant.

Information sharing is a concept that is a fairly new addition in doctrine, gaining in regular use starting in 2000 with Joint Vision 2020. Even though this is the case, information sharing has been a requirement and a precursor for successful operations throughout history. Information sharing currently enhances each tenet of the Command, Control, Communications, Computers, and Intelligence (C4I) concept as delineated in Table 9.

C4I Tenet	Information Sharing Enhancement
Command and Control	Allows the commander to make more effective decisions in planning, directing, coordinating, and controlling forces and operations by having better information available.
Communications	Expands the use of communications beyond voice. Information sharing leverages other media and data sources such as live or captured video, biometric data, historical analysis, and many others.
Computers	Puts computers capable of capturing, sharing, and receiving various media into the hands of those operating at the front line of conflict, where information is simultaneously most rich for collection and most immediately usable.
Intelligence	Information sharing gets more information in the hands of intelligence professionals for analysis. Furthermore, this additional analysis is also more easily shared back to the originator and other stakeholders.

Table 9. Information sharing enhances the concepts of C4I

It is important to understand that breakdowns in information sharing such as those regarding the 9/11 attacks in 2001, and the aftermath of Hurricane Katrina in 2005, have led to the execution of new strategic guidance and emerging technological capabilities, however it is only after a disaster these shortfalls are realized. After 9/11, the national storyline was dominated by asking why the government could not “connect the dots” to prevent the attack, and after Hurricane Katrina, the government was questioned by the mainstream media as to why various departments and agencies were unable to coherently work together during the response. These failures are reminders of the associated consequences of not sharing information, and when used as examples in concert

with the gains that could be made with implementation, present a compelling storyline to incite action towards greater government-wide information sharing.

The 9/11 attacks were the catalyst that caused the substantial changes in the intelligence community. Once the intelligence community became focused on information sharing, it was realized that there were not enough assets to handle all of the collection and analysis required. This realization spread into the military intelligence community and it was quickly realized that all forces could operate as collection assets as long as they were given the proper tools. When all forces started reporting intelligence in droves during OIF, fusion centers were created. Acting as hubs for collection information, these fusion centers were able to effectively catalog and analyze the incoming data. These fusion centers were then able to export various intelligence products to decision makers as well as directly feed timely intelligence to special operations forces. The fusion centers would not be successful, however, if there was not a myriad of forces on the ground conducting collection activities and subsequently sharing them.

B. IMPLEMENTATION

1. Current Implementation

Current U.S. Navy Riverine Forces only have a limited number of systems available that could be used for information sharing. The best system that is currently in use is the Blue Force Tracker (BFT). The BFT, along with a Global Positioning System (GPS) device, allows for the continuous broadcasting of the current position to other forces through the BFT system. BFT is equipped with integrated maps that overlay other units' positions, creating a mobile operational picture. BFT also has the capability for broadcasting messages such as text messages or standard reports, allowing units to communicate in near real time. During the stand-up of Riverine Squadron One, the RPBs that were received from the USMC had only a few boats equipped with working BFT. Beginning in 2007, the U.S. Navy started equipping boats with upgraded communications gear

by adding BFT to all boats and replacing the existing radio with the PRC-117F pictured in Figure 16. Even though the PRC-117F was an upgrade, its advanced capabilities such as sending data were not taken advantage of and were left unused.

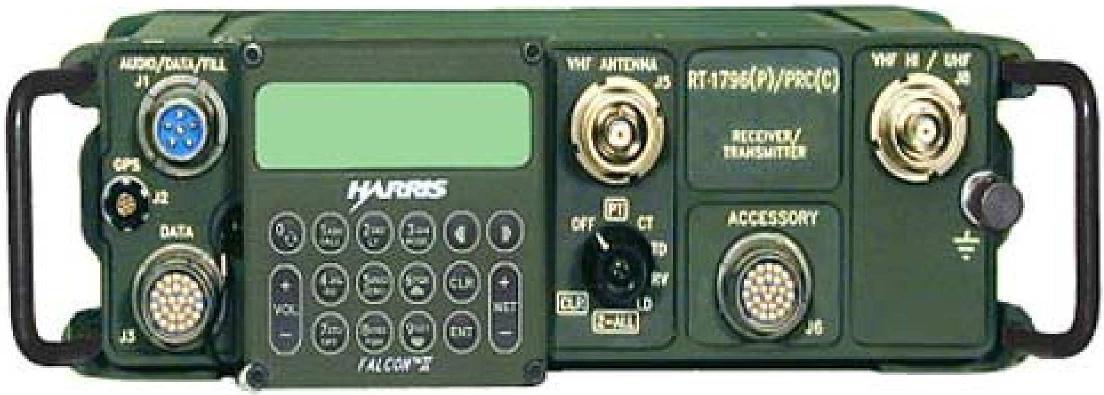

Figure 16. Harris AN/PRC-117F Radio (From Olive-drab.com, 2010)

The HQ element of the riverine squadrons also received the PRC-117F radio in order to maintain voice communications with operating forces, but did not receive BFT capabilities. This oversight resulted in a severely degraded capability, preventing the HQ element from executing command and control operation of riverine forces in near real time. The limited number of platforms available to conduct information sharing within the riverine squadrons, while new, are a result of requirements development that are not in line with the information sharing needs of the force. Because information sharing was mistakenly not a planned requirement for riverine forces, the ability to accomplish effective information sharing has been largely ineffective. Galli et al. (2007) argues that the original requirements only supported a narrow view of what a communications system should do. They also succinctly lay out that:

> The communications equipment in use by the riverine forces in tactical environments, though tried and proven in the field, is designed around dated military technologies that support a communications doctrine consistent with the periods they were developed. However, as time and technology have advanced, the

information demands of battlefield environments have grown to the point of dwarfing the capacities of legacy systems that seem to only be able to advance their capacity through lengthy development time and increased financial investment.

Information sharing has yet to be successfully and ubiquitously integrated at the tactical level for other forces operating in support of the current conflicts in Iraq and Afghanistan. BFT, pictured in Figure 17, represents the current best-of-breed of tactical information sharing. The DoD Information Sharing Implementation Plan (2009b) says of the current state: “While leadership is beginning to convey the importance of an information sharing culture, the need still remains to institutionalize information sharing behaviors.” In other words, currently, action and technology is lagging behind doctrine, policy and culture.

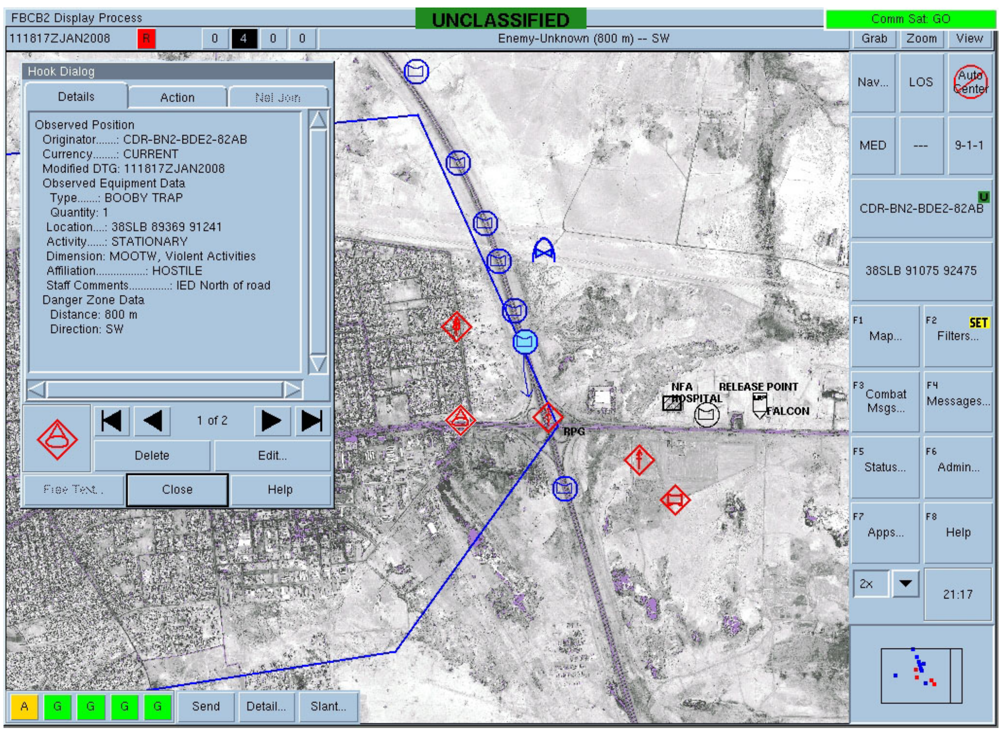

Figure 17. A Blue Force Tracker screen capture (From Kabis, 2008)

This is not to say that there has been no progress in the information sharing realm. The Combined Enterprise Regional Information Exchange System (CENTRIXS) network, used by many United States’ coalition partners, has expanded in use in Afghanistan and will soon out-number the amount of

Secret Internet Protocol Router Network (SIPRNET) terminals in many locations. It is billed by the DoD (2009b) as a “first step in converging the physically separated mission partner networks.” The most numerous attempts at comprehensive information sharing have been among partners during HA/DR operations. Tools such as Civil-Military Link (CIMILink), Peace Operations Support Tool (POST), Non-combatant Evacuation Operation Tracking System 2000 (NTS 2000), HarmonieWeb, and Relief Web are just a few that have been developed to meet this compelling need. Unfortunately, as the DoD (2009b) describes, consolidating these activities to a single tool or making tools work together is a difficult task, resulting in the situation that exists currently:

> The uncoordinated development of DoD’s various civil support and SSTR unclassified information sharing initiatives resulted in capabilities that are useful within their respective AORs, but are stovepiped and not federated for use across DoD or combatant command geographic boundaries. Specifically, the lack of a federated SSTR architecture hinders combatant commands and mission partners from efficiently and effectively sharing information in civil support and SSTR operations.

Information sharing tools, systems, and procedures have been effective in experiments and in limited application, so the next step for the DoD is to fund and implement these initiatives at the tactical level. In a recent white paper, Major General Michael Flynn (Flynn, Pottinger, & Batchelor, 2010), the senior intelligence officer in Afghanistan, said that it was essential to be able to:

> … integrate information collected by civil affairs officers, Provincial Reconstruction Teams (PRT), atmospherics teams, Afghan liaison officers, female engagement teams, willing non-governmental organizations and development organizations, United Nations officials, psychological operations teams, human terrain teams, and infantry battalions, to name a few.

The number of entities that would see gains in effectiveness through the use of information sharing tools far outnumbers what General Flynn mentions. Both tactical forces and the forces acting in a command and control function above them are looking for various capabilities that will help them. These include

getting updates on enemy activity and threat levels, receiving a real time operational picture of force locations and missions, passing on their availability for tasking, viewing unmanned systems feeds, as well as sharing gathered biometric data. These information sharing requirements expand beyond the United States' own forces as future operations will likely continue to be coalition focused. The Multinational Interoperability Council Concept Development and Experimentation Working Group (2008) states that for successful information sharing in future operating environments, "coalition forces will likely require the ability to:

- Share, access, and store information across strategic and operational domains;
- Obtain a comprehensive characterisation of all aspects of an operation (i.e., a network assessment) to include planning-related data, capabilities, restrictions, constraints, system connectivity, and interoperability information;
- Tailor joint, interagency, and multinational information displays to provide a real-time and accurate depiction of the operational area of interest;
- Fuse strategic level inputs such as intelligence and environmental information and operational level inputs from each of the environmental components (maritime, land, air, special forces, and logistics) into a tactical level common operating picture;
- Support tactical agility, effects orchestration, self-synchronisation, and distributed decision-making using a common operating picture."

The primary advantage that is sought with the use of information sharing capabilities is decision superiority. It is defined in Joint Vision 2020 (Shelton, 2000) as "better decisions arrived at and implemented faster than an opponent can react, or in a noncombat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission." Joint Vision 2020 also warns that decision superiority does not automatically come with information superiority, meaning that it takes more than an influx in information to make good

decisions. The missing piece that effective information sharing provides is the "unity of effort" that the U.S. JCS (2007) says is made possible by "close, continuous interagency and interdepartmental coordination and cooperation." The end result is that the tactical forces conducting operations, the operational level forces conducting command and control, and all other partners are more effective during operations. This effectiveness is described by the U.S. JCS (2009b) as being able to "accurately visualize the situation, anticipate events, and make appropriate, timely decisions more effectively than adversary decision makers."

2. Potential Implementation

As information sharing systems are integrated into riverine squadrons, many different roles of information collection, sharing, and utilization will take place within the different aspects of the squadron. These roles will differ in scope depending on the tasks assigned to the different portions of the squadron based on the needs of current operations.

The riverine squadron detachments would have the largest information sharing roles. The boat detachments are simultaneously the portion of the unit in the position to be most ably to collect information for sharing, while at the same time, the most in need of information from others to enable effective operations. Any systems implementation would have to treat these roles with equal weight. Like the BFT, information sharing systems should be installed on all boats to ensure that in whatever configuration is used for any particular mission, the situational awareness that is afforded is not degraded. Additionally, the interoperability between installed systems and the information sharing systems used by adjacent U.S. military units, as well as coalition partners must be a factor that is taken into account, but as the JCS (2009a) describes, "the most important requirements of this implication are frequent coordination and exercises with interagency and international partners and the development of common procedures before an occasion for commitment arises." As discussed in

Chapter IV regarding the Silver Fox, failure is imminent if systems are integrated without significant amount of time and resources devoted to training and exercising the operational use of those systems. Lastly, boat detachments must be able to receive targeted information from the riverine headquarters element, which plays a critical role in making sure operating boat detachments get the most relevant and critical information in real time.

The flexibility of riverine squadrons comes from their ability to seamlessly integrate various detachments of experts with special capabilities or systems. Past integration has included unmanned systems detachments, Naval Criminal Investigative Service (NCIS), combat engineers, Military Working Dogs (MWD), Explosive Ordnance Disposal (EOD), and many others. Each of these groups has their own information sharing requirements that will need to be utilized and integrated while attached to riverine forces. One effect this integration will have on all parties involved is the reduction of duplicate information. Instead of each entity on any given mission reporting on an event, such as the finding of a weapons cache, the entity with the most expertise, an EOD unit in this case, would be able to create the appropriate report while subsequently sharing it with all known and unknown interested third parties.

The last portion of the squadron with an information sharing role is the headquarters. There, the role of an information manager must be created. A watch position much like a Tactical Action Officer (TAO) on a U.S. Navy ship, the primary role would be to ensure detachments that are conducting operations are getting the information they need to be successful. Since there is a plethora of information available, the headquarters plays a key role in sifting through it and pushing forward information that is immediately useful to the detachments, allowing them to focus on the mission at hand and at only the most useful level of prevalent information, preventing them from being overburdened and distracted. The advantage that the headquarters element of the squadron has in this role is that they have much more available bandwidth, can focus on the larger area of

influence, and have the ability to tap into multiple other resources that the operating detachments may not have access to.

C. INFORMATION SHARING IN USE

Information sharing, as it becomes more prevalent throughout the U.S. military, is going to be found to be useful throughout various types of conflict and through the associated full range of that conflict. For stability operations specifically, the use of information sharing is discussed in the following three scenarios:

- Humanitarian Assistance/Disaster Relief
- Counterinsurgency
- Government and Security Force Development

1. Humanitarian Assistance/Disaster Relief

The U.S. JCS Joint Operating Concept for SSTRO contains a consolidated listing of the various objectives and associated capabilities that are required for the joint force commander to conduct these types of operations. Information sharing is specifically called out in this high-level joint document because it is apparent that it is critical to the success in the HA/DR mission via the objectives and capabilities listed in Table 10.

Objective	Capability
Provide unified action through joint command, control, and coordination	The ability to conduct seamless knowledge sharing among DoD elements, U.S. Government agencies, and multinational partners prior to, during, and after the completion of SSTR operations.
Deliver humanitarian assistance	The ability to coordinate and integrate with USG agencies and multinational organizations in order to support humanitarian assistance and disaster response efforts.

Table 10. HA/DR information sharing objectives and capabilities from (U.S. JCS, 2006)

One of the many challenges that are presented during HA/DR operations is that the diversity of all the different entities makes it difficult to have a concerted unity of effort. The DoD (2009b) expects that the groups will be wide-ranging, regularly being made up of "U.S. departments and agencies, foreign governments and security forces, international organizations, non-government organizations, and members of the private sector." Because the capabilities and needs of the various groups are very different, the likelihood that they are not aligned is unfortunately high. As Barge, Davis, and Schwent (2003) argue, this is a hurdle that must be overcome because "neither the military nor the civilian can function effectively without the other. They are interdependent … making information sharing essential for mission accomplishment." Information sharing would help these different entities pool resources and work more effectively together to prevent duplication of effort and enhance the focus of effort. This effort will only be able to be properly aligned when, as Benbow et al. (2006) lays out, "extensive planning, de-confliction, rehearsal, and coordination" are conducted. The strength of information sharing is that it is specifically designed

to be independent of whether the entities are physically near each other or not. This makes the prospect of aligning these groups much more feasible to do when preparing for the next HA/DR operation, which for the most part, is of unknown and random time and location. The DoD (2007) describes the result of this close coordination and preparedness as widely diverse units, that when called, are ready and able to "share information that promotes informed decision making, improves situational awareness, establishes economies of knowledge, and creates unity of effort."

An additional challenge that is presented during HA/DR operations is that the information needed to ensure success is both immense in scope and complicated in depth. The various entities supporting the operation will need information about population locations and vulnerabilities, conditions of infrastructure such as water, power, sewage, locations of aid sites and how much room for additional victims is available, locations where searches have and have not been conducted, as well as information about what actions other groups are taking. This is only a few of the many data points needed by operational planners, but as Bridges and Mason (2003) make clear, quantity of information does not equate to quality in this type of environment, and that if "reasoned choices" are to be made, they must be made with an emphasis on quality. The DoD Information Sharing Strategy (2007) defines this concept as "veracity":

> The ability to create relevance and de-conflict potentially conflicting data received from a number of sources. While analysts and decision-makers may receive more information, more quickly, and from more directions, its accuracy, consistency, authority, currency and completeness must be validated.

The way that the information needed to conduct operations can be made available to operating entities and validated is through information sharing. The complexity of the amount and depth of information involved and the scrutiny that must be applied argues for dedicated systems of much greater capability than currently fielded systems. Ahciarliu (2004) agues that these systems should

follow the Structured Humanitarian Assistance Reporting (SHARE) approach which lays out guidelines for achieving veracity that include:

- Geo-referenced information signifying where the data was collected, such as the latitude and longitude.
- A time-stamp, particularly important in fast-moving emergencies where information validity is relative to time, indicating when data was collected and at what frequency.
- Information about the data itself defining its credibility such as: the source of the information, the measurement standards and indicators used for the applied methodology.

Information sharing systems built with the SHARE approach will increase the capability of those making operational decisions, resulting in aligned priorities of effort, people that are rescued and cared for quicker, supplies that are distributed in a more targeted manner, and aid money that is spent wisely.

Riverine forces have a set of capabilities that are both unique and wide-ranging. The many types of activities that they could realistically be called upon to do during HA/DR operations include, but are not limited to, conducting search and rescue, transporting victims or refugees, completing surveys of infrastructure along the waterways, transporting supplies and materials, and providing movement for aid and recovery personnel. The U.S. JCS (2008) argues that in order for these types of capabilities to be taken advantage of by the various interagency, IGO, and NGO groups that are working beside one another, a collaborative environment must exist in which “participants share data, information, knowledge, perceptions, ideas, and concepts, often in real time regardless of physical location.” For the riverine forces, implementation of an information sharing capability allows for active participation in this role. This will allow the myriad of capabilities of the riverine forces to become known and offered, allowing various entities to leverage them. As Russo (2006) argues, this “seamless integration” of different groups, operating in support of common HA/DR objectives, “is essential to ensure that all of the combat and support elements can take advantage of one another’s strengths.”

In addition to having capabilities that can be leveraged, riverine forces are also an effective information gathering force. Their access to areas that are either unreachable, or not commonly traveled by most other units makes them uniquely capable to get information that others may not be able to gather, such as whether areas along waterways have been searched, conditions of port facilities, and waterway conditions for other craft. The advantage here lies not only with the fact that riverine forces are in a position that many other units cannot claim, but also that they are experts in the maritime domain. One of the mission areas that riverine forces were designed for is Maritime Domain Awareness (MDA), which Benbow et al. (2006) defines as an "understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States." This expertise, gained through the exercise of their MDA mission, allows the riverine forces to be the authoritative source on all information that is sought on maritime related issues. This maritime domain, which without riverine forces may be lacking due to lack of expertise, is an excellent opportunity for riverine forces in support of HA/DR operations to gather civil information, which the JCS (2009b) defines as "information developed from data about civil areas, structures, capabilities, organizations, people, and events that can be fused or processed to increase interagency, IGO, and NGO situational awareness."

2. Counterinsurgency

Contained in the U.S. JCS Joint Operating Concept for SSTRO are objectives and capabilities necessary for successful operations throughout the range of conflict those stability operations present. Included among these are specific objectives that put forth an argument that information sharing in the counterinsurgency portion of stability operations is a critical factor in attaining success. These objectives and capabilities are listed in Table 11.

Objective	Capability
Provide unified action through joint command, control, and coordination	The ability to conduct seamless knowledge sharing among DoD elements, U.S. Government agencies, and multinational partners prior to, during, and after the completion of SSTR operations.
Establish responsive battlespace awareness / understanding	The ability to tag, track, and localize hostile elements in all domains.

Table 11. Counterinsurgency information sharing objectives and capabilities From (U.S. JCS, 2006)

One of the primary tactics that insurgents use is making themselves inconspicuous by blending in with the populace. Insurgents' ability to do this successfully is because counterinsurgents do not have enough experience or information about normal activities of the populace they are operating amongst. This is a fundamental deficiency that must be overcome, because in order to achieve success on COIN operations, the U.S. JCS (2009b) instructs that, "comprehensive knowledge of the operational environment," is required. The primary method for counterinsurgent forces to combat this setback is to consistently operate among the people. These types of activities enable the opportunity to collect significant amounts of information to include data about the people, their activities, their desires and concerns. Flynn et al. (2010) describe this plethora of information as "vast and underappreciated" and say success lies in the counterinsurgents' ability to "acquire and provide knowledge about the population, the economy, the government, and other aspects of the dynamic environment we are trying to shape, secure, and successfully leave behind." This information gathering and sharing prevents insurgents from being able to take sanctuary among the populace, especially when human information gathering is coupled with other technologies such as biometric, signals, and unmanned systems information gathering. New and upgraded information

systems are necessary to handle the inclusion of these technologies because as Marvin (2005) describes, the information that needs to be shared, fundamental to mission success, has “rapidly overtaken the capability of low bandwidth, purely voice network capability.”

The second challenge that presents itself in a counterinsurgency environment is that the information that is most useful is found at the tactical level and shared up, which is the opposite that one would expect from conventional force-on-force conflict. The U.S. JCS (2009b) reasons that this is due to "the fact that all units collect and report information, combined with the mosaic nature of insurgencies.” Sharing of this tactical level data is extremely valuable at the operational level, where assessments of progress are discerned and decisions about focus of effort are made, because as Bridges and Mason (2003) describe, “decision makers both at the field and at headquarters level need quality and sufficient information to serve as a basis for making reasoned choices.” Getting the data from the lowest levels is very challenging, as at the tactical level, the unit is the most involved in day-to-day operations. Thus, at this level, they bear the predominance of the burden of both operating on received information, gathering information, and preparing it for sharing. Flynn et al. (2010) observed this information burden first hand in Afghanistan:

> At the battalion level and below, intelligence officers know a great deal about their local Afghan districts but are generally too understaffed to gather, store, disseminate, and digest the substantial body of crucial information that exists outside traditional intelligence channels.

Seamless integration of information systems will reduce the workload of these overburdened units. Sundland and Carroll (2008) describe the goal as being able to “collect, fuse, analyze, and disseminate information to decision makers to facilitate effective understanding.” Achieving this goal can allow for more informed decisions to be made at the operational and strategic levels.

Because of their expertise in the maritime domain, riverine forces are more easily able to differentiate between the local populace and insurgents using the waterways. For most units, it would be difficult to discern the difference between locals using the waterway for normal transit or commercial activity and the insurgents using it to transit around checkpoints or to transfer weapons and contraband to other sympathizers. In order to become well versed in being able to tell the difference between the local populace and insurgents, an intense amount of time on station, talking to locals who live along, or work on the waterway is required. Ryan (2007) says that this investment of both time and energy is warranted because “such interaction provides invaluable opportunities to gain insight into the local situation.” Additionally, the intensity in which information is gathered from the local populace on the waterway will act as a deterrent to insurgents who would otherwise seek to utilize it as an alternative to the more densely manned roadways. These encounters, when coupled with information sharing systems, allow for the collection, mining, and sharing of these nuances between units, allowing a much more enhanced capability to detect insurgents spread among other units that may not have in-person riverine support afforded to them. As Cross (2007) describes, this is a core capability of U.S. Navy forces, as “ultimately, MDA is about collecting and sharing large amounts of data and information.”

Riverine forces also provide an excellent tactical capability to gather information that can be useful at the operational and strategic levels. One of the biggest reasons that riverine forces can do this is because they have the ability to travel much longer distances than most ground units will during normal operations by traveling along the waterways. This method of travel allows riverine forces to travel between operating areas expeditiously, and at times, allows them the capability to provide support to multiple operating areas at the same time. This ability to maneuver with more freedom between operating areas affords them multiple advantages in the information domain. One advantage that is gained is that by having the same force supporting multiple operating areas is

that the information gathered, packaged, and sent to higher commands comes from one singular source. This ability satisfies what Rumsfeld (2006) described in the 2006 QDR when he said that what was needed was “increased situational awareness and shared information on potential threats.” Obtaining information from a singular source allows for less variability to exist in the information that is received, making the tasks that must be undertaken using this information much less subject to risks and uncertainty that come with variability in information reporting. Additionally, the riverine force’s ability to support numerous ground units in different areas of operation provides this unique capability to be spread throughout the battle space in a targeted fashion by operational leadership. As Hochstedler (2006) describes, this targeted capability increases the frequency in which information can be collected and allows operational commanders to “greatly increase the power to counter asymmetric threats in the maritime environment.”

3. Government and Security Force Development

To effectively accomplish government and security force development, various broad objectives need to be accomplished. Information sharing can play a large part in making these easier to accomplish, and hence speed up the development effort. Of the many objectives described in the U.S. JCS SSTRO JOC, the following objectives listed in Table 12 are ones that meet the goals of government and security force development and will likely benefit greatly from the increased use of information sharing.

Objective	Capability
Provide unified action through joint command, control, and coordination	The ability to conduct seamless knowledge sharing among DOD elements, U.S. Government agencies, and multinational partners prior to, during, and after the completion of SSTR operations.
Establish a representative, effective government and the rule of law	The ability to assist in the organization and training of personnel to work in the various government ministries and agencies.

Table 12. Government and security force development information sharing objectives and capabilities from (U.S. JCS, 2006)

Government development activities are very challenging because they involve a myriad of forces trying to advise the smallest and most basic units throughout the country. It many cases, the activities being developed are the same in the adjacent town, province, or operating area, but little information is available about the lessons learned regarding what has been working, what has not, and what resources are most needed to make the development mission a success in the shortest time possible. In addition to the goals and objectives of the training being the same, but disconnected, the training is further complicated by the various different entities conducting the training, which can range from special operations forces, regular forces of various services, international partners, to civilian contractors. This diverse group of trainers and mentors that are tasked with this development role face an uphill battle on maintaining commonality and consistency in the mentoring they provide. Information sharing systems would help this situation. The U.S. JCS (2007) calls this necessary coordination the “vital link” and touts many advantages to include the ability to “build international and domestic support, conserve resources, and conduct coherent operations that efficiently achieve shared goals.” Through the use of information sharing systems, efficiencies would be gained by using the best

practices discovered during operations, even though the operating areas may be disconnected by time or space. In the DoD (2009b) Information Sharing Implementation Plan, it says stability operations "necessitate interaction and information sharing with many external organizations." These systems would accomplish this by allowing for collaboration and detailed planning to take place between forces of different make-ups.

During security force development operations, brilliance in the basics is the primary focus of training. To move beyond this and achieve a level of expertise to a point whereby units can operate in support of one another requires skills and experience most times not found in newly established security forces. These forces will need to successfully operate among each other and in doing so, as Benbow et al. (2006) lay out, will "need to conduct extensive planning, de-confliction, rehearsal, coordination to avoid blue-on-blue casualties." Additionally, as a recruiting incentive during security force development operations, many new recruits are offered assignments to units near their home. While this is working well as a recruiting incentive, it provides an additional challenge to forces involved in security force development, as it is difficult to develop trust relationships between units that have little in common, or with forces that do not have a diversity of locations or life experiences to rely upon. These challenges present a problem that can be eased with the integration of information sharing systems into the developing forces. The DoD (2007) describes a culture of sharing as "a mindset where information is continually shared as a normal course of work." The implementation and integration of this culture early on in the training pipelines for these new security forces will foster a much more comprehensive approach to information sharing among disparate units and allow for cohesion to develop through integrated operations that would be difficult to otherwise create. It is also very likely that with being able to leverage the knowledge and assistance of other units, the speed in which units will reach a level of maturity and are capable of autonomous operations is likely to be significantly faster.

The ability to operate on waterways gives riverine forces the advantage of not being confined to a single operating area in many instances. This is a definitive advantage when it can be utilized, but in some cases this is not possible due to the nature of the waterway terrain. This waterway terrain limitation is not unique to riverine forces, as any government entity that riverine forces are conducting development with will have to adapt to the same limitations. There are various things that can prevent units from being able to take advantage of the entire waterway. For example, in Iraq, a dam, shallow water, and landlocked waterways that existed caused riverine forces to either not be able to operate on a continuous body of water, or even required separate deployment locations for riverine detachments. These types of limitations are annotated by the OSD (2005) as hindrances to the "speed, agility, and flexibility" needed to conduct operations. This instance, where the reach of riverine forces or government entities is limited, argues for the advantages gained by the use of information sharing systems to be leveraged to include what Cohen et al. (2006) explain as the increased ability to "make observations, draw lessons, apply them, and assess results." Information sharing will allow government entities that suffer from instances of physical disconnectedness to share lessons learned in developing their capabilities, making the maturity of the government development effort reach fruition with much more expediency and simultaneously preventing what Barge et al. (2003) describe as the "shortfalls, friction and redundancy of effort" that can develop otherwise.

Riverine forces are many times not used as the locus of effort, but serve as a support entity to operations taking place on land. This is a crucial mission area for riverine forces to teach to security forces. Coordination is challenging and requires seamless integration during both the planning and execution phases of operations. What can make this coordination even more challenging is attempting to do so during operations utilizing only tactical radio circuits. This type of coordination can be executed, but overcoming communication obstacles requires intense amounts of established common operating procedures, training,

and practice before being able to be successfully employed in an operational environment. The integration of information sharing systems can allow for a more comprehensive ability to work together in these challenging environments. The DoD (2007) argues that information sharing allows units to “achieve dynamic situational awareness and enhance decision making.” This type of advantage allows forces the ability to be adaptive and nimble in assisting each other when fast-moving situations present themselves, allowing for the most effective use of the capabilities on hand to be used at the correct time and place. Russo (2006) states that what is needed is “a common operating environment that seamlessly integrates all of the units involved.” This type of operating environment leads to close coordination, and when coupled with effective use of combat power, can promote legitimacy of the security forces among the population, as they become more effective at securing their country.

D. CONCLUSION

Information sharing is the critical factor that allows operational commanders to make the best decisions possible. The commander making these decisions, with the gains able to be made from information sharing, has more data, data of different types, and data from different sources, all of which are able to be used in concert with staff and field expertise to advise on the best course of action for any endeavor that stability operations may present. Riverine forces are only at the beginning stages of implementing information sharing systems, but as systems like the BFT are brought online and utilized during operations, the benefits are readily apparent and are easily assimilated into normal day-to-day operations. The ultimate goal is for leaders to be able to make better decisions, faster, especially in the realms of stability operations, and implementation of information sharing capabilities allows them to do exactly that.

In the following chapter, the discussions of biometric, unmanned, and information sharing systems will come together to describe a riverine force that is a much more dominant and effective force due to implementation of these new

technologies. The conclusion will also discuss how the riverine force is just one of many units conducting stability operations that could benefit from the same technological revolution that is proposed for the riverine force in this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. A NEWLY EQUIPPED NAVAL RIVERINE FORCE

Breaking from the mold of the 20th century paradigms that have defined today's U.S. Military make–up, a newly equipped riverine force would be equipped with the latest technology that would not expand its mission beyond what doctrine, publications, and instructions delineate, but would rather make those roles and responsibilities able to be accomplished in a much more effective manner. Stability operations are the fundamental mission the military must be prepared for in the 21st century, and the U.S. Navy Riverine Force is a unit that is capable and ready to perform its mission in this challenging arena.

Riverine forces are able to fill a critical gap between where traditional land and maritime forces can effectively operate. Because these areas are so important and are home to significant segments of the population, they can also serve as a key operational area during stability operations. While this is where the riverine force strength lies, its disadvantages must be compensated for. The current disadvantages that greatly increase operational risk include a reduced capability to engage the population, reduced situational awareness, and limited communication reach-back capability. These limitations fundamentally make the riverine force mission a more dangerous one, adding risk that is unnecessary and correctable.

Compensating for and correcting these risks involves improving the technological capability of the riverine force in three tiers: biometric, unmanned, and information sharing systems. These improvements will have a significant effect throughout the range of operations that riverine forces will be tasked to operate in. As was argued in Chapter I, the most likely situation that riverine forces will be called upon to address in the future is going to be stability

operations, in which humanitarian assistance and disaster relief, counterinsurgency, and government and security force development will constitute the crux of what is tasked.

Navy Riverine forces play a unique role in HA/DR scenarios because they are able to access different areas of terrain that are otherwise not accessible due to various reasons. This access provides the operational commander the ability to utilize riverine forces to assess the condition of the affected area using unmanned systems, access key population centers to begin biometric profiling, and to begin to share data and inferences using information sharing systems. This allows the lead forces to prepare the terrain for additional organizations such as NGO's and IGO's, mitigating possible duplication of effort, and immediately leveraging the capabilities of the various support organizations when they arrive. Ultimately, this integration leads to a more expeditious search and rescue effort, seamlessly leading to follow-on rebuilding endeavors.

One of the most basic tasks riverine forces have during counterinsurgency operations is to execute patrols and immerse themselves amongst what is almost always the center of gravity, the people. This access to the terrain, both physical and human, allows riverine forces to conduct TSE to include biometric profiling, use of unmanned systems to enhance situational awareness, and participate in both the collection and sharing of critical information with both adjacent units and operational commanders. This information that is gathered and shared helps prevent insurgents from being able to take sanctuary among the populace. As one would expect, better decisions are consistently made when those who need it receive more accurate and timely information, and riverine forces can play a critical role in both the collection and use of this important data.

The instructing of foreign waterborne forces has been a staple mission of the riverine force for decades. The challenge of government and security force development requires steady advances in capacity and capability in order to gain the confidence of the population. Riverine forces are able to accomplish both of these through the training of the local government or security force that would

conduct enforcement of policy or law on the waterways. With riverine force assistance, the developing units will learn the utilization of biometrics to enhance their ability to understand the population, unmanned systems to focus effort on the people rather than on mundane tasks able to be accomplished otherwise, and information sharing in order to reap the benefits of lessons learned and pool resources. This development, with a culture of sharing information embedded early on, can allow these government entities and security forces to establish early effectiveness and gain trust and confidence from the people of their country.

B. IMPLICATIONS FOR THE JOINT FORCE

This thesis has put forth the argument that U.S. Navy Riverine forces can be aptly equipped with advanced technology, resulting in a drastic increase in capability for a relatively low cost. This situation is not unique to the riverine forces. Many of the arguments presented here are based on the unique characteristics of the riverine force or their capability to operate in an environment few others can, but these recommendations for the equipping of these technologies find merit in many other units throughout the joint force. While it may seem intuitive, the DoD would not create units that are no different than others in terms of their operational mission, or provide no advanced capability than their predecessor. Therefore, it must be understood that each unit is unique, operating on a unique landscape, with unique capabilities. When these are brought to bear, and combined with the rest of the joint force, it creates an overlapping and all-encompassing fabric of military capability. What the technologies in this thesis provide for the joint force is not a new piece to this fabric, but a higher “stitch count,” if you will, making the joint force more effective, efficient, and resilient in the capabilities they exercise than previously capable. It should be understood that for the most part, almost every unit that has operated outside of the wire in Operation Iraqi Freedom or Operation Enduring Freedom is likely a prime candidate to be supplemented with biometric, unmanned, and

information sharing systems, if they have not been already. Doing so accomplishes the advances in capability already discussed, but in a manner that takes into account the realities of the fiscal environment that usually follows long periods of extended conflict. Large, high cost, or long duration weapon system acquisitions are going to be difficult to argue for, so the focus of the joint force in the post-war years should be on resetting the force, updating the equipment, and training for future conflict.

As was mentioned in Chapter I, the future conflict the United States can expect to be involved in is likely to mirror the conflicts in Iraq and Afghanistan. The reason behind this is because, from the perspective of opposition forces, pulling the United States into a protracted and unconventional conflict is simply the most effective way to simultaneously wear down the military power and public support needed for the United States to participate in that type of conflict. While not all stability operations are caused by actions of opposition forces, i.e., natural disasters, the ones that are will be inspired by lessons from the conflicts in Iraq and Afghanistan. While the U.S. may ultimately prevail in those conflicts from the U.S. perspective, it will simultaneously be a modern lesson for unconventional forces on how to wage 21st century war against the United States. It only makes sense to prepare for this type of conflict by strengthening the ability to work more cohesively among our own forces and with the forces of the allies of the United States. Implementing biometric, unmanned, and information sharing systems with those goals in mind and with an understanding of what 21st century conflict will bring may not be as staunch a deterrent as 20th century weapons systems, but will serve as systems that can and will be used to make the inevitable warfighting and disaster response a much less costly endeavor in terms of time, money, and lives.

C. RECOMMENDATIONS

This thesis purposely did not explore in depth the technical requirements for the implementation of the various information technology systems that were argued for. Further research would be very advantageous to type and system commands that are exploring options for the integration of various IT systems, especially within the riverine force. Specifically, how new systems will be able to utilize or leverage existing communication architecture is of critical importance. Also of importance is upgrading the communications architecture to 802.16 to be able to handle the increasing amount of data that will need to be sent during operations. Additional research could be done into how the integration of the IT systems mentioned in this thesis could be incorporated into NECC as whole to make the concept of adaptive force packaging more of a reality. Also of interest is how NECC forces will deploy and operate when large-scale conflicts do not exist and stability operations continue to be the predominant type of operation that is conducted. The most likely way to do this is by leveraging U.S. Navy amphibious ships and NECC sea bases. This would require IT upgrades to those platforms as well, which would be another instance in which further research is necessary. Lastly, NTTP 3-06.1 Riverine Operations mentions that if multiple riverine squadrons were deployed at one time, the Riverine Group would be required to take operational control of the forces in theater. Unfortunately, Riverine Group One is not properly equipped for this eventuality, nor is NECC headquarters equipped to operationally control any NECC adaptive force packages. Further research that would be very valuable would be a study into what IT resources would be needed to be able to accomplish the appropriate command and control functions from these headquarters. Processes, procedures, command and organizational structures will likely need to be examined as well.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Ackerman, R. K. (2007). Riverine challenges mirror joint operations. *Signal.* Retrieved October 10, 2010 from Fairfax, VA: AFCEA Signal Online: http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1351&zoneid=210

Ahciarliu, C. M. (2004). *Multi-agent architecture for integrating remote databases and expert sources with situational awareness tools: humanitarian operations scenario.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Aho, B. (2006). *Iraqi soldier assigned to Iraqi riverine police force.* Retrieved September 16, 2010 from Washington, DC: United States Department of the Navy: http://www.navy.mil/view_single.asp?id=40455

Barge, H., Davis, M. S., & Schwent, J. T. (2003). *Field level information collaboration during complex humanitarian emergencies and peace operations.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Beaver, J. W., Mercado, P. R., Bucher, A .D., Free, J. M., Byers, R. W., & Oliveria, T. V. (2006). *Systems analysis of alternative architectures for riverine warfare in 2010.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Benbow, R., Ensminger, F., Swartz, P., Savitz, S., & Stimpson, D. (2006). *Renewal of Navy's riverine capability: A preliminary examination of past, current and future capabilities*. Retrieved November 13, 2009 from Fort Belvoir, VA: Defense Technical Information Center: http://handle.dtic.mil/100.2/ADA447820

Biometrics Identity Management Agency. (2009). *Biometric use cases.* Retrieved March 8, 2010 from Washington, DC: Biometrics Identity Management Agency: http://www.biometrics.dod.mil/References/biometricusecases.aspx

Biometrics Task Force. (2008). *Biometrics task force annual report FY2008.* Retrieved March 8, 2010 from Washington, DC: Biometrics Identity Management Agency: http://www.biometrics.dod.mil/Files/Documents/AnnualReports/fy08.pdf

Bridges, D. M. &, Mason, A. R. (2003). *Exploring of wireless technology to provide information sharing among military, United Nations and civilian organizations during complex humanitarian emergencies and peacekeeping operations.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Boraz, S. C. (2009). Maritime domain awareness: Myths and realities. *United States Naval War College Review, Summer 2009.* Retrieved March 4, 2010 from Newport, RI: United States Naval War College: http://www.usnwc.edu/getattachment/26abc82e-a497-4933-9bbc-67881e714c3d/Maritime-Domain-Awareness--Myths-and-Realities---S

Boyd, J. M. (2008). New handheld device meets maritime challenge. *The Biometric Scan, Volume 4, Issue 1.* Retrieved March 8, 2010 from Washington, DC: Biometrics Identity Management Agency: http://www.biometrics.dod.mil/Newsletter/issues/2008/Jan/v4issue1_pm.html

Boyd, J. M. (2009). *Navy contributions to identity management.* Presentation delivered at the Biometric Consortium Conference, Tampa, FL. Retrieved March 11, 2010 from Fort Meade, MD: The Biometric Consortium: http://biometrics.org/bc2009/presentations/tuesday/Boyd_NAVY%20BR%20A%20Tue%201117-1126.pdf

Bush, G. W. (2006). *National Security Strategy of the United States of America* Retrieved October 3, 2009 from Washington, DC: White House Archives: http://georgewbush-whitehouse.archives.gov/nsc/nss/2006/nss2006.pdf

Cartwright, J. E. (2009). *2009 Joint Professional Military Education (JPME) Special Areas of Emphasis (SAEs).* Retrieved December 5, 2009 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/doctrine/education/sae_2009.pdf

Cassidy, R. M. (2004). Back to the street without joy: Counterinsurgency lessons from Vietnam and other small wars. *Parameters, 34.* Retrieved March 3, 2010 from Carlisle Barracks, PA: U.S. Army War College: http://www.carlisle.army.mil/usawc/Parameters/Articles/04summer/cassidy.pdf

Center for Army Lessons Learned. (2008a). *Military police and counterinsurgency operations: Operation Iraqi freedom initial impressions report (IIR).* Retrieved February 4, 2010 from George Town, Grand Cayman: Public Intelligence: http://info.publicintelligence.net/MP_COIN_OpsIIR-CDR-4045.pdf

Center for Army Lessons Learned. (2008b). *Tactical site exploitation.* Retrieved September 6, 2010 from Fort Leavenworth, KS: United States Army Combined Arms Center: http://usacac.army.mil/cac2/call/thesaurus/toc.asp?id=29093

Climate Change Science Program (CCSP). (2008). *Analyses of the effects of global change on human health and welfare and human systems*. A Report by the U.S. Climate Change Science Program and the Subcommittee on Global Change Research. [Ebi, K.L., Sussman, F.G., Wilbanks T.J., Gamble, J.L. (Eds.)]. Retrieved December 11, 2009 from Washington, DC: U.S. Environmental Protection Agency: http://cfpub.epa.gov/ncea/cfm/recordisplay.cfm?deid=197244

Cohen, E., Crane, C., Horvath, J., & Nagl, J. (2006). Principles, imperatives, and paradoxes of counterinsurgency. *Military Review, March-April 2006.* Retrieved December 5, 2009 from Fort Belvoir, VA: Defense Technical Information Center: http://handle.dtic.mil/100.2/ADA486811

Cordesman, A. H. (2004). *The "post-conflict" lessons of Iraq and Afghanistan.* Retrieved November, 15, 2009 from Washington, DC: Center for Strategic and International Studies: http://csis.org/files/media/csis/congress/ts040519cordesman.pdf

Cordesman, A. H. (2005). *The Iraq war and its strategic lessons for counterinsurgency.* Retrieved November 15, 2009 from Washington, DC: Center for Strategic and International Studies: http://csis.org/files/media/csis/pubs/050912_countinusrg.pdf

Cross, E. C. (2007). *Modern advances to the Modular Fly-Away Kit (MFLAK) to support maritime interdiction operations*. Master's thesis, Naval Postgraduate School, Monterey, CA.

Deady, T. K. (2005). Lessons from a successful counterinsurgency: The Philippines, 1899-1902. *Parameters, 35.* Retrieved October 27, 2009 from Carlisle Barracks, PA: U.S. Army War College: http://www.carlisle.army.mil/usawc/Parameters/Articles/05spring/deady.pdf

Defense Information Systems Agency. (2010). *Introduction to the defense information systems agency campaign plan.* Retrieved March 13, 2010 from Arlington, VA: Defense Information Systems Agency: http://www.disa.mil/campaignplan/campaignplan2010.pdf

Department of Defense. (2008). *Department of defense biometrics enterprise strategic plan 2008-2015.* Retrieved March 12, 2010 from Washington, DC: Department of the Army Biometrics Task Force: https://secure.biometrics.dod.mil/Home/Files/20080827_DoD_Biometrics_Enterprise_Strategic_Plan.pdf

Department of Defense Directive Number 3000.07. (2008). *Irregular Warfare.* Retrieved January 22, 2010 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/whs/directives/corres/pdf/300007p.pdf

Department of Defense Directive Number 8220.02. (2009). *Information and Communications Technology (ICT) Capabilities for Support of Stabilization and Reconstruction, Disaster Relief, and Humanitarian and Civic Assistance Operations.* Retrieved January 22, 2010 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/whs/directives/corres/pdf/822002p.pdf

Department of Defense Instruction Number 3000.05. (2009). *Stability Operations.* Retrieved November 13, 2009 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/whs/directives/corres/pdf/300005p.pdf

Director, Navy Staff. (2005). *Implementation of Chief of Naval Operations (CNO) Guidance Global War on Terrorism (GWOT) capabilities.* Retrieved January 29, 2010 from Monterey, CA: Homeland Security Digital Library: https://knxas1.hsdl.org/?view&doc=48077&coll=0

Duhan, D. P. (2005). *Tactical decision aid for unmanned vehicles in maritime missions.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Faram, M. D. (2008). CO: Riverines must stay close to Marines. *Navy Times.* Retrieved October 8, 2010 from Springfield, VA: Navy Times: http://www.navytimes.com/news/2008/04/navy_riverines_042708w/

Ferebee, J. M. (2009). *Maximizing situational awareness: improving situational awareness with global positioning system data in the maritime environment.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Flores, R. A. (2007). *Improving the U.S. Navy riverine capability: lessons from the Colombian experience.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Flynn, M. T., Pottinger, M. F., & Batchelor, P. D. (2010). *Fixing intel: A blueprint for making intelligence relevant in Afghanistan.* Retrieved March 8, 2010 from Washington D.C.: Center for a New American Security: http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf

Freitas, M., & Treadway, B. W. (1994). *Stygian myth: U.S. riverine operations against the guerilla.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Galli, M., Turner, J. M., & Olson, K. A., Mortensen, M. G., Wharton, N. D., Williams, E. C. . . . Shan, O. W. (2007). *Riverine sustainment 2012*. Retrieved October 27, 2009 from Fort Belvoir, VA: Defense Technical Information Center: http://handle.dtic.mil/100.2/ADA469560

Galula, D. (1964). *Counterinsurgency warfare: Theory and practice.* New York, NY: Praeger.

Gates, R. M. (2010). *Quadrennial defense review report.* Retrieved March 4, 2010 from Washington, DC: United States Department of Defense: http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf

Hedderly, J. W. (2008). *A seakeeping study on the autonomous sustainment cargo container delivery system.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Hochstedler, R. A. (2006). *Implementation of a modular Fly Away Kits (FLAK) for C4ISR in order to counter asymmetric threats in the coalition riverine and maritime theatres.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Hodge, N. (2009). U.S. Struggles with 'Electronic Fratricide' in Afghanistan. *Wired*. Retrieved October 8, 2010 from New York, NY: Wired: http://www.wired.com/dangerroom/2009/11/us-struggles-with-electronic-fratricide-in-afghanistan/

Hom, A. R. (2008). The new legs race: Critical perspectives on biometrics in Iraq. *Military Review, January-February 2008.* Retrieved March 12, 2010 from Fort Leavenworth, KS: United States Army Combined Arms Center: http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20080228_art013.pdf

Hunt, A. F. (2010). *Lance Corporal Maxx A. Juusola.* Retrieved August 10, 2010 from Montreal, Quebec: Zero Anthropology: http://zeroanthropology.net/2010/07/06/the-killing-fields-of-marja/

Insitu. (2010). *Integrator backgrounder.* Retrieved October 8, 2010 from Bingen, WA: Insitu: http://www.insitu.com/documents/Insitu%20Website/Marketing%20Collateral/Integrator%20Backgrounder.pdf

Jennings, K., & Chan, Y. (2005). *Applications of biometrics in mass disaster victim identification.* Retrieved March 3, 2010 from East Lansing, MI: Michigan State University Department of Computer Science and Engineering: http://www.cse.msu.edu/~cse891/Sect601/CaseStudy/BiometricsDisasterVictimID.pdf

Jennings, T. (2009). *Department of defense biometrics program overview*. Presentation delivered at the Armed Forces Communication and Electronics Association Monthly Luncheon, Fort Belvoir, VA. Retrieved March 13, 2010 from Bethesda, MD: Armed Forces Communication and Electronics Association, Belvoir Chapter: http://www.afceabelvoir.org/userdocuments/SpeakerPresentations/AFCEABelvoirDoDBiometricsPMBriefing10282009.pdf

Johnson, S. E. (2005). *Deployable Network Operations Center (DNOC): A collaborative technology infrastructure designed to support tactical sensor-decision maker network operations.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Junker, D. B. (2008). *Office of Naval Research (ONR) Maritime Domain Awareness (MDA) vision*. Presentation delivered at the Maritime Security and Domain Awareness Conference, San Diego, CA.

Kabis, B. (2008). *Blue force tracker screen capture.* Retrieved November 11, 2010 from Laughlin Air Force Base, TX: Laughlin Air Force Base News: http://www.laughlin.af.mil/news/story.asp?id=123082048

Kelley, S. W. (2005). *An analysis of the use of medical applications required for complex humanitarian disasters and emergencies via Hastily Formed Networks (HFN) in the field.* Master's thesis, Naval Postgraduate School, Monterey, CA.

LaFranci, H. (2001). Rivers: the last frontier in coca war. *The Christian Science Monitor.* Retrieved October 12, 2009 from Boston, MA: The Christian Science Monitor: http://search.csmonitor.com/durable/2001/06/12/p6s1.htm

Lim, M. H., & Ng, M. Y. C. (2007). *An integrated architecture to support the Hastily Formed Network (HFN).* Master's thesis, Naval Postgraduate School, Monterey, CA.

Marvin, C. E. (2005). *802.16 OFDM rapidly deployed network for near-real-time collaboration of expert services in maritime security operations.* Master's thesis, Naval Postgraduate School, Monterey, CA.

McCoy, K. M. (2009). *Naval sea systems command overview.* Presentation delivered at the 14th Annual Expeditionary Warfare Conference, Panama City, FL. Retrieved March 13, 2010 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/ndia/2009expedition/mccoy.pdf

McCurry, M. C. (2006). *Riverine force—A vital Navy capability for the Joint Force Commander*. Retrieved October 27, 2009 from Fort Belvoir, VA: Defense Technical Information Center: http://handle.dtic.mil/100.2/ADA463522

McNamee, W. (2010). *Earthquake evacuees await rescue.* Retrieved July 10, 2010 from Washington, DC: National Geographic Society: http://news.nationalgeographic.com/news/2010/02/photogalleries/100202-haiti-earthquake-pictures/#/haiti-earthquake-leaving-boats-port_12576_600x450.jpg

McQuilkin, W. C. (1997). *Operation Sealords: A front in a frontless war, an analysis of the brown-water Navy in Vietnam.* Master's thesis, Army Command and General Staff College. Fort Leavenworth, KS.

Mercado, A. (2008). *Exploring data sharing between geographically distributed mobile and fixed nodes supporting Extended Maritime Interdiction Operations (EMIO).* Master's thesis, Naval Postgraduate School, Monterey, CA.

Mullen, M. G. (2009). *CJCS guidance for 2009-2010.* Retrieved February 1, 2010 from Washington, DC: Joint Chiefs of Staff: http://www.jcs.mil/content/files/2009-12/122109083003_CJCS_Guidance_for_2009-2010.pdf

Multinational Interoperability Council Concept Development and Experimentation Working Group. (2008). *Future coalition operating environment: Interoperability challenges for the future—Version 3.0.* □ Retrieved December 17, 2009 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/futurejointwarfare/concepts/futurecoalitionevnv3.doc

Naval Air Systems Command. (2010). *DON awards STUAS contract. Retrieved from* Patuxent River, MD: Naval Air Systems Command: http://www.navair.navy.mil/pma263/stuas/stuas_contract_Award.pdf

Navy Expeditionary Combat Command (2010). *Riverine force fact sheet.* Retrieved December 13, 2010 from Virginia Beach, VA: Naval Expeditionary Combat Command: http://www.public.navy.mil/usff/necc/Documents/RIVERINE_FactSheet%20-%202010%20v2.pdf

O'Rourke, R. (2006). *Navy role in Global War on Terrorism (GWOT) — Background and issues for Congress*. Retrieved January 30, 2010 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA479030

O'Rourke, R. (2009). *Navy role in irregular warfare and counterterrorism: Background and issues for Congress*. Retrieved January 30, 2010 from Fort Belvoir, VA: Defense Technical Information Center: http://handle.dtic.mil/100.2/ADA501330

Office of Naval Research. (2009). *Silver Fox UAV.* Retrieved October 8, 2010 from San Francisco, CA: Wikimedia: http://commons.wikimedia.org/wiki/File:Silver_Fox_UAV.jpg

Office of the Secretary of Defense. (2005). *Unmanned aircraft systems roadmap 2005-2030.* Retrieved March 17, 2010 from Washington, DC: Federation of American Scientists: http://www.fas.org/irp/program/collect/uav_roadmap2005.pdf

Office of the Secretary of Defense. (2009). *Unmanned systems integrated roadmap 2009-2034.* Retrieved March 17, 2010 from Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics: http://www.acq.osd.mil/psa/docs/UMSIntegratedRoadmap2009.pdf

Olive-Drab.com. (2010). *Harris AN-PRC 117F.* Retrieved November, 9, 2010 from Calabasas, CA: Olive-Drab.com: http://www.olive-drab.com/od_electronics_anprc117.php

Oliver, G. (2008). *Security, stability, transition, and reconstruction operations* [Video]. Newport, RI: United States Naval War College.

Paquin, K. R. (2009). *Use of conventional U.S. Naval Forces to conduct FID in Colombia.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Phang, N. S. (2006). *Tethered operation of autonomous aerial vehicles to provide extended field of view for autonomous ground vehicles.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Quarles, E. L. (2008). *An analysis of collaborative technological advancements achieved through the Center for Network Innovation and Experimentation.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Rumsfeld, D. H. (2006). *Quadrennial defense review report.* Retrieved August 23, 2009 from Washington, DC: United States Department of Defense: http://www.defense.gov/qdr/report/report20060203.pdf

Russo, J. A. (2006). *Test and evaluation of meshdynamics 802.11 multi-radio mesh modules in support of coalition riverine operations.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Ryan, M. (2007). The military and reconstruction operations. *Parameters, 37.* Retrieved March 3, 2010 from Carlisle Barracks, PA: U.S. Army War College: http://www.carlisle.army.mil/usawc/Parameters/Articles/07winter/ryan.pdf

Sasser Jr., & W. E. (2007). *AFRICOM: The U.S. Navy's emergent missions and capability gaps*. Retrieved November 30, 2009 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA470726

Shedd, D. R. (2009). *Quadrennial intelligence community review.* Retrieved February 24, 2010 from Washington, DC: Federation of American Scientists: http://www.fas.org/irp/dni/qicr.pdf

Shelton, H. H. (2000). *Joint vision 2020.* Retrieved August 20, 2009 from Washington, DC: United States Forest Service: http://www.fs.fed.us/fire/doctrine/genesis_and_evolution/source_materials/joint_vision_2020.pdf

Snow, K., Harris, D., & Adhikari, B. (2010). Haiti Relief: Anger Mounts Among Desperate Haitians Over Supplies Stuck at Airport. *ABC News.* Retrieved October 14, 2010 from New York, NY: ABC News: http://abcnews.go.com/WN/HaitiEarthquake/haiti-earthquake-tensions-mount-supplies-stuck-airport/story?id=9573873&page=1

Spangler, D. J. (1995). *What lessons can be drawn from U.S. riverine operations during the Vietnam War as the U.S. Navy moves into the twenty-first century.* Master's thesis, Army Command and General Staff College, Fort Leavenworth, KS.

Speer, G. D. (2002). *US Colombia Policy: What's Next?* (Statement before the Senate Subcommittee on Western Hemisphere, Peace Corps, and Narcotics Affairs). Retrieved October 24, 2010 from Washington D.C.: U.S. Senate: http://dodd.senate.gov/press/Speeches/107_02/0424-speer.htm

Stavroulakis, G. (2006). *Rapidly deployable, self forming, wireless networks for maritime interdiction operations.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Stolzenburg, M. A. (2008). *Unified vision for the future: Riverine squadrons and the security cooperation MAGTF.* Master's Thesis, Army Command and General Staff College, Fort Leavenworth, KS.

Stone, A. (2009). *Military patrol boat.jpg.* Retrieved January 10, 2010 from San Francisco, CA: Wikimedia: http://commons.wikimedia.org/wiki/File:Military_patrol_boat.jpg

Stubbs, B. B., Clapp, E. (2009). Navy moving forward with tactical (biometric) identity management system. *Defense Daily.* Retrieved March 20, 2010 from Washington, DC: DoD Executive Agent for Maritime Domain Awareness: http://www.dodeaformda.navy.mil/contentview.aspx?id=634

Sundland, J. J., & Carroll, C. J. (2008). *Transforming data and metadata into actionable intelligence and information within the maritime domain.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Telegraph. (2010). Haiti earthquake: 400,000 to be resettled outside Port-au-Prince. *Telegraph.* Retrieved June 30, 2010 from London, United Kingdom: Telegraph Media Group: http://www.telegraph.co.uk/news/worldnews/centralamericaandthecaribbean/haiti/7048954/Haiti-earthquake-400000-to-be-resettled-outside-Port-au-Prin ce.html

Tomes, R. R. (2004). Relearning counterinsurgency warfare. *Parameters, 34.* Retrieved March 3, 2010 from Carlisle Barracks, PA: U.S. Army War College: http://www.carlisle.army.mil/usawc/Parameters/Articles/04spring/tomes.pdf

Towell, P. (2009). Defense: FY2010 authorization and appropriations. *Congressional Research Service.* Retrieved January 29, 2010 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA511913

United Nations Children's Fund. (2009). *Tsunami report: Five year anniversary.* Retrieved September 17, 2010 from New York: United Nations Children's Fund: http://www.unicef.org/media/files/UNICEF_Tsunami_5yr_Report_Final.pdf

United States Army and United States Marine Corps Counterinsurgency Center. (2009). *Situation report.* Retrieved February 17, 2010 from Fort Leavenworth, KS: Unites States Army Combined Arms Center: http://usacac.army.mil/blog/cfs-filesystemfile.ashx/__key/CommunityServer.Components.PostAttachments/00.00.00.61.08/AUG-09-SITREP.pdf

United States Department of Defense. (2007). *Information sharing strategy.* Retrieved October 30, 2009 from Washington, D.C.: Department of Defense: http://cio-nii.defense.gov/docs/InfoSharingStrategy.pdf

United States Department of Defense. (2008). *National defense strategy of the United States of America*. Retrieved October 12, 2009 from Washington, DC: Department of Defense: http://www.defense.gov/news/2008%20national%20defense%20strategy.pdf

United States Department of Defense. (2009a). *Quadrennial roles and missions review report.* Retrieved October 8, 2010 from Washington, D.C.: Department of Defense: http://www.defense.gov/news/Jan2009/QRMFinalReport_v26Jan.pdf

United States Department of Defense. (2009b). *Information sharing implementation plan.* Retrieved October 30, 2010 from Washington, D.C.: Department of Defense: http://cio-nii.defense.gov/docs/DoD%20ISIP%20-%20APR%202009_approved.pdf

United States Department of the Navy. (2006). *Navy transformation*. Hearing before the Readiness Subcommittee of the Committee on Armed Services, House of Representatives. Retrieved February 19, 2010 from Washington, DC: US Government Printing Office: http://www.gpo.gov/fdsys/pkg/CHRG-109hhrg10933793/pdf/CHRG-109hhrg10933793.pdf

United States Department of the Navy. (2008). *NTTP 3-06.1 Riverine Operations.* Newport, RI: Naval Warfare Development Command.

United States Government Accountability Office. (2004). *Information security: Technologies to secure federal systems.* Retrieved January 22, 2010 from Washington, DC: United States Government Accountability Office: http://www.gao.gov/new.items/d04467.pdf

United States Joint Chiefs of Staff. (2001). *Joint publication 1-02: Department of defense dictionary of military and associated terms*. Retrieved November 1, 2010 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

United States Joint Chiefs of Staff. (2004). *National military strategy of the United States of America.* Retrieved October 12, 2009 from Washington, DC: Department of Defense: http://www.defense.gov/news/mar2005/d20050318nms.pdf

United States Joint Chiefs of Staff. (2006). *Military Support to Stabilization, Security, Transition, and Reconstruction Operations Joint Operating Concept (JOC).* (Version 2.0). Retrieved November 1, 2009 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/futurejointwarfare/concepts/sstro_joc_v20.doc

United States Joint Chiefs of Staff. (2007). *Joint publication 1: Doctrine for the armed forces of the United States*. Retrieved November 1, 2009 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/doctrine/new_pubs/jp1.pdf

United States Joint Chiefs of Staff. (2008). *Joint publication 3-0: Joint operations*. Retrieved November 1, 2009 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf

United States Joint Chiefs of Staff. (2009a). *Capstone concept for joint operations* (Version 3.0). Retrieved November 1, 2009 from Norfolk, VA: Joint Forces Command: http://www.jfcom.mil/newslink/storyarchive/2009/CCJO_2009.pdf

United States Joint Chiefs of Staff. (2009b). *Joint publication 3-24: Counterinsurgency operations*. Retrieved November 1, 2009 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/doctrine/new_pubs/jp3_24.pdf

United States Joint Chiefs of Staff. (2010). *Joint publication 3-10: Joint security operations in theater*. Retrieved March 13, 2010 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/doctrine/new_pubs/jp3_10.pdf

Verett, M. J. (2006). *Performance and usage of biometrics in a testbed environment for tactical purposes.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Volger, A. (2006). *ArcGIS.* Retrieved October 22, 2010 from Zurich, Switzerland: Swiss Federal Institute of Technology: http://www.photogrammetry.ethz.ch/research/heli/mais.html

Waterfield, B. (2010). Haiti earthquake: 10,000 buried each day in mass graves. *Telegraph.* Retrieved June 30, 2010 from London, United Kingdom: Telegraph Media Group: http://www.telegraph.co.uk/news/worldnews/centralamericaandthecaribbean/haiti/7045722/Haiti-earthquake-10000-buried-each-day-in-mass-graves.html

Watkins, M. B. (2005). *DOD 050906-N-6436W-408*. Retrieved October 13, 2010 from Sunnyvale, CA: Yahoo! Inc.: http://www.flickr.com/photos/39735679@N00/691140672/

Willey, P. F. (2004). *The art of riverine warfare from an asymmetrical approach.* Master's thesis, Naval Postgraduate School, Monterey, CA.

Wilson, B. (2009). *N851 naval special warfare branch.* Retrieved February 27, 2010 from Fort Belvoir, VA: Defense Technical Information Center: http://www.dtic.mil/ndia/2009expedition/Wilson.pdf

Woodward Jr., J. D. (2005). Using biometrics to achieve identity dominance in the global war on terrorism. *Military Review.* Retrieved March 20, 2010 from Rand Corporation: *http://www.rand.org/pubs/reprints/2006/RAND_RP1194.pdf*

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Dan Boger, Chairman, Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

4. Professor Glenn Cook, Associate Chairman
   Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

5. Professor R. Mitchell Brown III
   NWC Monterey Program
   Monterey, California

6. Dr. Karl Pfeiffer, Assistant Professor, Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

7. Commander, Fleet Forces Command
   Norfolk, Virginia

8. Commander, Naval Expeditionary Combat Command
   Norfolk, Virginia

9. Commander, Riverine Group One
   Norfolk, Virginia

10. Commanding Officer, Riverine Squadron One
    Norfolk, Virginia

11. Commanding Officer, Riverine Squadron Two
    Norfolk, Virginia

12. Commanding Officer, Riverine Squadron Three
    Yorktown, Virginia

13. OPNAV N851
Washington, DC

14. PEO, Littoral and Mine Warfare
Washington Navy Yard, DC

15. Commanding Officer, Center for Security Forces
Norfolk, Virginia

16. Commanding Officer, USCG Joint Maritime Training Center
Camp Lejeune, North Carolina

17. Commanding Officer, Expeditionary Combat Readiness Center
Virginia Beach, Virginia

18. Commander, Maritime Expeditionary Security Group One
San Diego, California

19. Commander, Maritime Expeditionary Security Group Two
Portsmouth, Virginia

20. Commander, Amphibious Squadron Eight
Norfolk, Virginia

21. Vice President and Director, Advanced Technology & Systems Analysis
Center for Naval Analysis
Alexandria, Virginia

22. Commander, Surface Warfare Development Group
Norfolk, Virginia

23. Commander, Dahlgren Division Naval Surface Warfare Center
Dahlgren, Virginia

24. Commander, Port Hueneme Division Naval Surface Warfare Center
Port Hueneme, California

25. Commander, Carderock Division Naval Surface Warfare Center
West Bethesda, Maryland

26. Director, Carderock Division Naval Surface Warfare Center, Detachment Norfolk
Norfolk, Virginia